14－H003

# 情報化社会におけるリスクとJRMS

## －リスク対策検討委員会 調査研究報告書－

平成１５年３月

JIPDEC

財団法人　日本情報処理開発協会

KEIRIN

この資料は、競輪の補助金を受けて作成したものです。

# 序

ユビキタス社会といわれるようＩＴ環境の進展には著しいものがある。情報環境の進化に応じ情報機器を利用する側においても格段の変化が見られるようになった。まさに変化こそ恒常的である。

とりわけ、コンピュータの利用については、機器そのものもさることながら、ネットワークを通した利用が増大し、便利さの反面、不正アクセス、コンピュータウイルスの作用が加速度的に増大し、ネットワークに関するセキュリティを重視せざるをえなくなってきた。

2002 年には金融機関において生じた情報システム障害の社会の様々な部面に与えた影響の大きさが着目され、情報システムに関わるリスクマネジメントの重要性が再確認された。こうした情報環境におけるリスク対応のため、2002 年３月に発表された「JIPDEC リスクマネジメントシステム（ＪＲＭＳ）のあり方に関する研究（ＪＲＡＭ2002)」の有効性を判断するための作業が必要となってきた。企業経営に関わる環境変化に目を向け、その実態をまとめ、さらに情報システムとセキュリティに関する動向を洗い出す作業を通して、情報セキュリティの現状を把握することにした。

現実の企業経営にＪＲＭＳを適用する場合、その有効性を検証するため、実証実験を行う必要性がある。実証実験への協力企業を得て、質問票に対する回答の仕方・集計結果の出し方など、使いやすさに関わる情報を入手することができ、実証実験の結果、リスク対策検討委員会ではＪＲＭＳの質問項目それ自体にメスを入れることになった。

本報告書では、最近の経営環境に関わる一般的な変化、情報セキュリティに関する動向、実証実験の結果を踏まえや見直し作業の結果が示されている。特に、ＪＲＭＳ質問票の新しいバージョンを含めている。そこでは、旧バージョンにおける回答者グループにも見直しが行われている。しかし、全体で約 1,000 項目近い質問からなるＪＲＭＳであるが、完全なバージョンであるとはいいがたい。むしろ、情報システムに依存する現場では、バックグランドの異なる担当者が質問項目に対し修正・改善を見出すことが多々あると思われる。当協会としては、社会的な有効性をできるだけ高めることが重要であると考えている。ＪＲＭＳがさらに現実的で利便性・有効性の高いプログラムとなり、リスク対応の最適化に資することを期待している。

なお、本調査研究報告書の取りまとめ等にご協力いただいた、リスク対策検討委員会委員、実証実験の協力くださった企業に心から謝意を表します。

2003 年３月

財団法人日本情報処理開発協会

# 2002年度リスク対策検討委員会

（敬称略／五十音順）

委員長　森宮　　康　　明治大学　商学部教授

委　員　池内　正英　　安全工学（株）　代表取締役社長

笠間　誠一　　(株)日立製作所　金融システム事業部金融ソリューションシステム本部　第一部

指田　朝久　　東京海上リスクコンサルティング（株）危機管理グループ主席研究員

花香　俊明　　ハナカリサーチセンター　代表

原田　要之助　　(株)情報通信総合研究所　情報流通プラットフォーム研究グループグループリーダー／エグゼクティブリサーチャー

松原　榮一　　ガートナージャパン（株）ジャパンリサーチセンターマネージングディレクター

# 目　　次

# 1．経営環境の変化とリスク

ユビキタス社会といわれるようにコンピュータに依存する度合いが増している今日、経営環境における情報システムの変化はきわめて著しい。その背景にあるのは情報システムを利用する組織の活動にある。問題は、そうした活動にリスクが内包されていることである。それだけに影響を受ける組織や人々にとり、あらためてリスク対応の必要性を喚起せざるを得ないのが現状であるといえる。

とりわけ、経営活動を考慮する場合、理論的にも実践的にも環境対応の意味に重要な変化が生じてきている。従来の展開では、各部門において目標値を設定し部門の最適化が全体に資するといった視点から、「部分最適」を指向する傾向が強かった。しかし、個々の部門において最適化を求めても、それが必ずしも全体にとって望ましいとはいえないことが理解されるようになった。いわゆる「全体最適」の視点である（Eliyahu Goldratt & Jeff Cox[1992]The Goal, The North River Press Publishing Corporation,エリヤ・ゴールドラット著、三本木亮訳[2001]『ザ・ゴール』ダイヤモンド社）。

全体最適の追及に関しては、さまざまな制約要因に目を向けなければならない。これまでも、全体と部分に関するシステム論は展開されてきたが、組織において個々の部門だけでは機能し得ない。全体との相互依存関係のもとで経営目標を達成するという方向性がなくてはならない。この点の鍵を握るのが情報であるが、情報システムの進展、特にネットワークを通して部門間の統合がこれまで以上に意味をもつようになったといえる。

この点の重要性は、全体最適にとりいかなるリスクが制約要因になるかである。たとえば、各部門には部門固有のリスクがあり、その顕在化は個々の部門だけの問題ではすまない。リスク対応にあたっては全体への影響を考慮することが前提となる。それだけに、組織とともに情報システムに関わるリスクについての理解が重要である。全体最適のためにはリスクマネジメントによるリスク対応が不可欠であり、ＪＲＭＳは組織活動に関わるリスクへの対応を支援するシステムとして意義を有しているのである。

以下は、当委員会においてＪＲＭＳの質問項目の見直し作業を行った際に確認された環境変化の一端である。

## 1.1　リスクに関する社会的変遷

リスクに対する人々の意識は社会環境の変化により確実に変化してきた。企業規模が大であることがさまざまなリスクに対する信頼の尺度であった時代もあった。しかし、相対的に大であった企業が最悪の問題状況である経営破綻に陥り、企業規模に対する信頼は終焉した。量的な尺度から、小規模でもリスクに対する耐性のある安定的な企業に信頼が置かれるように変化したのである。企業としてリスク耐性の優れた安定性を有していることが重要な要件となったわけであり、信頼の尺度が質に移行するに至った。

しかしながら、現実に企業なり組織の統合が業種により進められており、情報システムはそれにより巨大化している。巨大なシステムダウンについては、1997年８月の東京証券取引所の株式

売買システムダウンがあり、2002 年４月にはみずほ銀行の決済システムの障害事故が発生した。また、2003 年３月には航空管制用飛行計画処理システムがダウンし、「航空会社の損害 10 億円」といった記事がでた（出典：日本経済新聞、2003 年３月５日）。単に企業が結合し規模を拡大したとしても、それだけではステークホルダーは満足しなくなったのである。ましてや利便性を重視するようになった時代背景の中で、金融機関等におけるシステム障害により、たとえば、キャッシュカードによる取引ができなくなることだけで由々しい問題となる。システム障害の原因が何であれ、システム間の接続が適切に行われず、取引が正常に行われなくなれば、顧客は不便さと共に当該金融機関等に対し不信感を抱く結果となる。さらに、商品開発等のシステムの運用に関する戦略にも影響が及ぶ。

情報社会ではシステムの利用の仕方も重要な意味を有するようになってきている。それによりネットワークの利用に関係する犯罪の形態も変化してきた。たとえば近年の傾向としては、かつてのショベルカーによるＡＴＭの破壊、金融機関・現金輸送車襲撃といった形態とは異なる、ネットワークを利用した金融機関からの現金詐取のケースもでてきている。

また、ネットワークに接続された情報システムでは、コンピュータウイルスによりシステム障害が発生し、その影響が関係者に広く連鎖していくのである。たとえば、ワームによる汚染の連鎖の速度が経営に与える影響も考慮しなければならない。2001 年に猛威を振るった Code Red worm の場合、世界のコンピュータのホストに感染するのに 12 時間かかったと言われているが、2003 年の Sapphire worm の場合、10 分以内とされた。その影響については、単に個々の組織の問題を超え、国における情報システムのセキュリティインフラストラクチャの面も考慮しなければならないことになる。

概して、従来、企業ではシステム障害に関して伝統的な自然災害等を除けば、外部からの作用を発生原因として想定する傾向があり、不正アクセスなりウイルスへの対応を重視してきた。しかし、内部のシステム開発・運用業務に関わるオペレーショナルリスクの影響がいかに経営にとり大きなものであるかが明らかになった。いずれにしても、現代の組織にあってはシステムへの依存度は高く、情報システムに関わる問題は情報システム部門のみではなく、経営陣やユーザ部門に作用することを前提として考えなければならない。

さらに、個人情報に関する問題も注視すべきである。この点については問題の一部には漏洩があるが、それも文書のみならず電子媒体、さらにネットワークを介在することになった。これらはすべからく「人」のモラルハザードが介在する問題である。

情報システム以外にも「人」が関わったケースとしては、経営陣のみならず現場担当者のモラルハザードを重視しなければならない事態が発生してきた。とりわけ、金融市場における経営陣のモラルハザードに関わるケースでは経営陣の行動が取り上げられた。政治の世界での不正献金や経営情報の不正利用によるインサイダー取引・横領・不正取引等が発生し、経営者に対しコーポレートガバナンスが着目されるに至った。アメリカでも、問題の性質は異なるが、エンロン、ワールドコムといった企業で経営に関わる人のモラルが問われる事態が出来した。いずれのケースでも、問題が顕在化してから事後的に対応せざるをえなかった。モラルハザードに関わる問題の背景には、組織として経営情報をリスクの点から理解することのなさと、情報開示に関わるリスクコミュニケーションの不十分さなり、チェック機構の不備に起因する傾向が強い。

最近の傾向には、経営のトップではなく、現場の担当者が介在するケースが目立つ。原子力発

電所における物理的ハザードの情報隠し、狂牛病に関わる食品会社での現場における偽装表示等はモラルハザードに関わるケースであった。このような内部／外部からの告発に端を発したケースもあるが、昨今では企業内部の通報制度の開設に関する動きも出てきている。

これらの側面に対し、関係諸機関・団体が何もしてこなかったわけではない。対応のすべてをここで明示することはできないが、その一端を示しておきたい。アメリカでは企業の一連の不祥事に対して1992年に内部監査の枠組みがＣＯＳＯ（The Committee of Sponsoring Organizations of the Treadway Commission）により提示された。欧州でも1980年代以降、コーポレートガバナンスが指向され、ＯＥＣＤ（Organization for Economic Cooperation and Development）でも企業行動に関するコードを提示してきた。金融機関に対してはＢＩＳ（Bank of International Settlements）も検査基準を示してきた。ロンドン証券取引所でもリスク情報の開示を義務づけてきている。また、アメリカではアンダーセンが介在したエンロン、ワールドコムの経営破綻を契機に2002年に企業改革法（Sarbanes-Oxley Act）が登場した。

### 1.1.1　アメリカにおける企業改革法とコーポレートガバナンス

アメリカの企業改革法は日本でも着目されている。内容的にはまだ不明確な面も含まれているが、経営情報、監査法人、倫理コード等に関し重要な特徴がある。経営情報に関しては、公開会社の財務諸表等に対しては経営を担うＣＥＯ、ＣＦＯの証明が必要とされた。すなわち、Section 909では、公開会社の財務諸表を含む定期的な報告書類等に対してはＣＥＯ、ＣＦＯが真正であることを証明しなければならないこととなった。また、1934年証券取引法により記録書類が同法に遵守していないことを知りつつ証明を行った場合には、刑事上罰則が科されることになる。

公開会社の財務諸表を監査する監査法人の監督機関（Public Company Accounting Oversight Board）が設置されることになった（Section　101（ｄ））。その構成員は５人（Section　101（ｅ））とされ、そのうち２名は公認会計士（１名は就任前５年間、監査法人のＣＥＯに就任していないこと）で、任期は５年（２期を超えることはできない）、兼職は禁止とされた。

さらに監査を実施する監査法人の義務が明記されている（Sections 201～）。そして、監査法人は監査業務以外禁止されることになった（Section 201（ａ））。特に、監査を行う監査法人は監督機関に登録し、登録監査法人（Registered Public Accounting Firm）となり、未登録の監査法人が監査報告書作成に関係することは違法であるとされている（Section 102（ａ））。公開会社は監査委員会（Audit Committee）を設置し、承認を受ける（Section　202）が、監査委員会を設置しない場合には取締役会が監査委員会とみなされることになる（Section　205）。公開会社の監査委員会は監査法人の選定、報酬・監督について責任を負うことになり、監査委員会の構成員は取締役会のメンバーで、独立している（社外である）こと（コンサルティングフィ等を受領していない等）（Section 301）が明示された。

経営情報のディスクロージャに関しては、特にその範囲が拡大された（Sections 401～）。たとえば、日本でも取り上げられている特定目的会社（ＳＰＥ、ＳＰＶ、ＳＰＣ）については報告の義務が取り上げられ（Section　401）、情報開示にはオフバランス取引（Section　401）や定期的な報告書類（Section　401（ａ））が含まれ、しかも重要事項が真実であり、重要事実が削除されておらず、業績予想が企業会計原則に基づき示された財務・事業結果と一致していることの開示（Section　401（ｂ））も定められている。なお、オフバランスシートの開示については証券取引

委員会（ＳＥＣ）が調査し、議会に報告する（Section 401（c））ことまで規定されている。

その上、証券アナリストの利益相反も重視され、証券取引関連の団体（National Exchanges and Registered Securities Associations）は、研究リポートでエクィティを推奨するアナリストについて利害の衝突（利益相反）に関するルールを制定しなければならない（Section 501）ことになった。また、違反した場合の刑事責任（Titles 8～）についても規定されており、連邦調査を妨げたりする意図で報告書類等を破壊、変更、偽造すること（Section 802）、監査人が監査等記録を５年間保存しなかった場合（Section 806）、公的な利用のための書類の利用可能性を妨げるための変更、破壊、隠蔽すること（Section 1102）も対象となる。内部告発者（Whistleblower）が出るような事態も想定し、その者の権利・回復・保護の拡大が明示されている。たとえば、不正経理・会計操作等について情報を提供する従業員の行動に対して、経営者は解雇なり、嫌がらせ、また差別的な扱いをしてはならないという禁止条項（Section 806）が規定されたのである。

いずれにしても、重要なのは経営上の倫理であり、最高経営責任者（ＣＥＯ）に対して、報告書類の中に、ＣＦＯ、コントローラ、ＣＡＯ等に関する倫理コードを採択しているか否かを記載するよう求めている。なお、倫理コードについては、利害の衝突が生じた場合の倫理的な扱い、定期的な報告書類において正確・公正・タイムリーな開示を促進させることが要請されている。

エンロン事件、ワールドコム事件等のアメリカにおける企業不祥事に関わる市場混乱の原因について、日本経済新聞が 2002 年８月に行った「日本経済新聞社による企業の信頼性回復に関する調査」（115 社に調査票、回答は 101 社）の結果が報道された。

表１－１．アメリカの企業不祥事・市場混乱の主たる原因

| | |
|---|---|
| 私利私欲に走った経営者 | 45 |
| 目先の利益･過度の成長を求めた株主 | 20 |
| チェック機能を果たさなかった監査法人 | 15 |
| 不正を見抜けなかったＳＥＣ | 0 |
| 企業に偏った投資判断をしたアナリスト | 0 |
| その他 | 21 |

（出典：日本経済新聞、2002 年９月２日）

そこにおける問題状況には、経営者に対する厳しい目が確認できる。また、日本が信頼を回復し、企業統治を進展させるには何をなすべきかについては、以下の結果であった。

表１－２．日本が信頼回復・企業統治の向上ですべきこと

| | |
|---|---|
| 監査法人に対する監査の強化 | 67 |
| 不正会計等に対する刑事罰の強化 | 56 |
| アナリスト業務の中立 | 51 |
| 会計ルールの厳格化 | 34 |
| 告発者の保護強化 | 24 |
| 社外取締役が過半 | 4 |
| その他 | 3 |

（出典：日本経済新聞、2002 年９月２日）

日本においてもこのところ商法が数次にわたり改正されてきており、2003年４月の改正商法の施行により、アメリカ型の委員会等設置会社が登場する。そこでは取締役会は経営の監督を行い、日常業務は取締役会が選任する執行役員により行われる。また、取締役会は社外取締役が過半数とする３名以上により構成される「指名委員会」、「報酬委員会」、「監査委員会」からなり、従来の監査役は廃止されるのである。すでに30社前後が委員会等設置会社への移行を表明していると言われている（出典：日本経済新聞、2003年３月５日）。また、2003年には27年ぶりに公認会計士法の大改正が予定されており、企業との癒着に起因した粉飾決算により失われた信頼回復を目指すことになるが、これもコーポレートガバナンスに深く関係している。

これらに共通する基本的な側面は、企業としての情報の重要性とその適切な開示といえる。しかし、いかなる状況においても、基本的に重要なのは、企業としてどこに視点をおいて展開してきたかである。たとえば、市場や顧客の視点にたてば「顧客満足（ＣＳ）」の度合いが指標となる。組織を構成する従業員等についての「教育・訓練」が不可欠である。また、ステークホルダーの視点から企業の存続は前提であろう。いずれにも応え得なかったケースでは、残念ながら経営上、リスクの観点が不在であった。リスクとその影響を認識するには、経営環境の変化それ自体がリスクを発生させる要因であることを十分に理解することが不可欠なのである。

## 1.2　みずほ銀行システム障害

### 1.2.1　情報システムリスクの経営へのインパクト

情報システムに関するリスクを考える上で、2002年４月に発生したみずほ銀行のシステム障害は、われわれに大きな教訓を与えた。その経緯については新聞等に報道されているが、みずほ銀行のホームページにもその詳細が掲載されている。「今回のシステム障害の発生原因、再発防止策とお客様からの信頼回復に向けて」の全文は、ホームページを参照していただくとし、その概要は次のとおりであった。(http://www.mizuhobank.co.jp/company/release/news020619.html)

障害の概要

４月１日から新システムの稼働を開始したが、次の３つの障害が発生した。

（１）口座振替の事務処理遅延

みずほ銀行における口座振替の手続が遅延し、これによりみずほ銀行およびみずほコーポレート銀行での引落処理が遅延した。この結果、電力会社等の収納企業口座への入金や、収容企業への引落結果データの引き渡しも支払い期限を越えて遅延した。また、この事務処理遅延の混乱の中で、口座からの二重引落しが発生した。

（２）ＡＴＭ障害

４月１日と８日に、みずほ銀行のＡＴＭオンラインシステムに障害が発生し、デビットカード、コンビニＡＴＭ等も含めたキャッシュカード取引の一部が取り扱いできなくなった。この際、現金が未払いにも拘らず通帳に引落しが記載される支払誤記帳が発生した。

（３）振込遅延等その他の障害

その他に、みずほ銀行およびみずほコーポレート銀行で振込遅延、取立手形関係の遅延、外為事務処理の遅延等も発生した。

これらにより、全体として約半月間に300万件以上の処理に影響があった。これは、日本の金融機関のシステム障害としてはこれまでにない規模のものであり、特に障害の規模と継続した期間が長かったため、顧客が一時的に不便を被ったというレベルにとどまらず、預金者や取引企業の信用に大きな影響を与えた。(たとえば、「マイボイスコムの調査結果として、預金者の15%が銀行口座の変更等の対策を取っている。」(出典：日本経済新聞、2002年6月7日)) また、公共企業やクレジット会社が顧客に領収書を二重に発行したことなどに対する損害賠償額も、10億円を越えると推定された。

しかし、経営から見た時に一番大きなインパクトがあったのは、システム統合の時期が遅れたことにより企業合併の戦略的な目標を達成できなくなったことである。1999年8月の合併発表時には、システム統合により三行で合わせたシステム投資額の1,500億円を先進的なＩＴ活用に向け、海外金融機関と同レベルのシステムを構築する計画であった。これにより、他の国内金融機関に対し、ＩＴ活用による差別化を実現するはずであった。しかし、このシステム障害により、システム統合は当初計画より2年遅れた2004年4月から段階的に開始し、2004年末に完全な統合を予定している。つまり、2004年末までは別々のシステムを使用せざるを得ないので、業務面での統合を行い、人員を戦略的な部門に投入することにも制約が発生する。さらに、この期間に新しい金融商品等を開発しようとすると、それに必要なシステム機能追加は稼働させているすべてのシステムに対して行い、かつシステム統合時にはその内の一つを除き廃棄するため、システム投資の効率を低下させる。これらにより、先進的なＩＴ活用による戦略的な差別化は非常に難しくなった。

特に、このケースに先立ち、2002年1月に発生したＵＦＪ銀行のシステム障害と対比して考えると、経営にとってのシステムの重要度が浮き彫りになってくる。三和銀行と大和銀行が合併したＵＦＪ銀行では、2002年1月15日の合併当初からシステムを統合してサービスを開始した。しかし、1月28日に公共料金やクレジット料金の口座引落しで18万3,000件の二重引落しが発生した。この障害は発生当時としては、これまでの日本の金融機関で発生した最大のシステム障害であった。しかしこの障害は翌1月29日には解決し、統合されたシステムでのサービスが継続された。そして、統合されたシステムが稼働したことにより業務面での統合も可能となり、支店の統廃合も容易になったと考えられる。つまり、ＵＦＪ銀行のシステム障害は、企業合併の戦略的な目的達成には大きな悪影響を与えなかった。

この二つのケースから導かれる結論は、情報システムのリスクはすでに経営戦略の実現において考慮すべき必須の項目となっている、ということである。

一方、2001年1月にバーゼル銀行監督委員会 (Basel Committee on Banking Supervision) は、金融機関のリスク管理について、オペレーショナルリスクとして情報システムのリスクを含めた新しいフレームワーク (The New Basel Capital Accord) を発表した。
(関連URL; http://www.bis.org/のトップページから'New Basel Capital Accord'で検索すると、関連ドキュメントのPDFファイルのダウンロードが可能である。)

この新しいフレームワークは2006年からの適用が予定されているが、金融機関の総自己資本比率規制（これまでは、国際業務を行う銀行においては８%）について、信用リスクに加えてオペ

レーショナルリスク（コンピュータ障害、ドキュメントの不備、不正行為による損害）をカバーすることが必要になった。つまり、理論的には情報システムリスクの高い金融機関は、リスクに対応する総自己資本の積み増しが必要となる。そして、オペレーショナルリスクの大きな要素として情報システムのリスクが挙げられているが、その内容はこれまでは災害や機器故障によるシステムの停止、不正アクセスやコンピュータウイルスによる被害といった、組織の外部からのリスクを主に考えていた。しかし、今回のみずほ銀行のシステム障害は、システム開発やシステム運用という本来のシステム業務に内在するリスクが非常に大きいことを示す結果となった。

1.2.2　みずほ銀行システム障害の原因

みずほ銀行システム障害の主な項目として、①口座振替の事務処理遅延、②ＡＴＭ障害、③振込遅延等その他の障害が挙げられているが、それぞれの原因について次のように解明されている。

（１）口座振替の事務処理遅延の原因

口座振替の事務処理遅延の主要な原因として、次の４点が挙げられている。

①ＭＴ交換テーブルの不備

移行作業の事前準備において、口座振替システムにおける重要な役割を果たすＭＴ交換テーブルに誤った情報が入力されていた。このテーブルには、口座振替に係わる委託者（収納企業等）名、収納企業が持ち込む媒体の種類、ファイル数といった収容企業別に作業に必須の情報が入れてあるが、その内容に不備があったために正しい処理が行われなかった。

②スケジュールトランズの不備

スケジュールトランズは口座振替システムのデータ入力作業や返却作業など作業工程を管理するデータで、振替予定日などの情報が登録される。このデータ入力作業での誤りと、プログラム設計の問題により、エラーが発生した。

③ＪＣＬの不具合

口座振替作業のＪＣＬで、正しくセットされていないものがあった。

④受付事務処理の混乱

口座振替のテープを収納企業から受け取る業務で使っているシステムで、事前準備で登録した情報に誤りがあったり、店番の処理について途中で仕様を変えたことにより、受付事務の混乱が発生し、エラーの発生につながった。

（２）ＡＴＭ障害

2002年４月のシステム稼働では、勘定系のシステムは統合せずに、既存システム間の連携を行うグローバルプロセッサを経由してトランザクションの処理を行っていた。このグローバルプロセッサのプログラムに不具合があったために、この障害が発生した。

（３）振込遅延等その他の障害

コンピュータプログラムの品質が不十分でエラーが残っていたこと、新事務フローへの事前の訓練不足等により事務処理ミスが発生したことにより、振込遅延等の障害が発生した。また、大量事務処理を支えるシステムの機能付加や事務インフラの整備が不十分だったことも事務の混乱を招いた。

1.2.3　みずほ銀行システム障害の教訓

今回のみずほ銀行システム障害は、システム開発の段階にその原因が作られ、本番稼働時に障害が露呈するシステム開発トラブルの典型的なケースである。(例;稼働までに発見されなかったプログラムエラー)　これについて、『今回のシステム障害の発生原因、再発防止策とお客様からの信頼回復に向けて』では、次のようにその原因を分析している。

（1）各種テストやリハーサル等の事前準備の不足

コンピュータプログラムや事務の不具合は、各種テストやリハーサル等の事前準備が十分でなかったことによる。特に、口座振替システムについては、システム開発スケジュールの遅れから、テストが未了ないし不完全なものにとどまっていた。また、テストが完全に終了していないことも報告されていなかった。

（2）システム統合プロジェクト管理体制の不備

システム・事務の品質が不十分なままシステムを稼働する結論を下したのは、システム統合プロジェクトの管理体制が不完全で、障害部分の開発を行ったシステム開発部門から経営者に対して適切な報告が行われなかったためである。その原因として、システム開発部門のシステムに対するリスク認識・評価が不十分であったことが挙げられる。この結果として、システム開発部門から経営会議に対し、「残った一部課題も解決目処が立っており、予定どおり移行に臨む」旨の報告があり、これに基づいてシステム稼働の結論を下した。また、内部監査部門のシステム開発部門に対する外部からのチェック機能は、システム障害のリスク認識が不十分だったために行われなかった。

システム障害のリスクを減少させるためには、現実に起きた障害の背景にある障害発生の根本原因を解明し、それに対する対策を行わないと形をかえて別の障害が発生する。今回の障害原因分析では、障害を引き起こした直接的な要因として、次の４点が挙げられている。

・ＭＴ交換テーブルの不備
・スケジュールトランズの不備
・ＪＣＬの不具合
・受付事務処理の混乱

しかし、公開された資料では、これらの一次的な原因を引き起こした背景の原因については述べられていない。つまり、ＭＴ交換テーブルの不備であれば、なぜそれを引き起こしたのかについては述べられていない。(たとえば、入力ミスがあったが、それをチェックする手続きがなかった。では、なぜ入力ミスのチェックをする手続きが設けられなかったのか？）もちろん、社内の資料には述べられていることと思うが、障害原因の因果関係を徹底的に分析することが障害を発生させる根本の原因を解消し、障害対策をモグラ叩きゲームにしないために必要である。

今回のみずほ銀行システム障害のケースにより、賢明な経営者は情報システムのリスクが経営的にも大きなリスクになったことを実感した。その実感が不十分な経営者にはリスク担当部門(企業によっては、情報システム部門）が警鐘を鳴らすべきである。そして、経営者の、自社の場合はどの位のリスクがあるのかという質問に対し、その答えを作るプロジェクトを用意する。ここで「答えを用意する」のではないことに注意する必要がある。なぜなら、どの位のリスクがあるか

の答えを作れるのはリスク担当部門単独では不可能である。つまり、システム障害がビジネス面にどの位の悪影響を与えるかという分析は、業務を主管しているユーザ部門しかできない。実は、各企業はこれに似たプロジェクトを行った経験があるはずである。たとえば、阪神大震災や2000年問題の時、自社のシステムが停止した時のビジネスへの影響度分析はかなりの企業が実施した経験を持っている。これらの経験を活かして、システム障害のビジネスに対する影響度分析をユーザ部門を巻き込んで実施すべきである。

この分析を行うと、自社の業務がシステムに依存している度合いが高いことに多くのユーザ部門は驚くことになる。この情報を社内で共有することがリスク管理の第一歩であり、今回のケースのリスク管理についての最大の教訓である。

## 1.3 航空管制システム障害

### 1.3.1 航空管制システム障害の概要

2003年3月1日午前7時に、国土交通省が管理している「飛行計画情報処理システム」（ＦＤＰ）に障害が発生し、システムのサービスが約1時間中断した。ＦＤＰは、飛行計画情報を集中的に処理し、管制に必要なデータを管制官に提供するとともに、レーダー画面に便名等を表示するために飛行計画情報を関連システムに送信するものである。このシステムが停止したことにより、約20分間、全国各空港からの航空機の離陸が停止され、その後も出発便の間隔を通常より長くする出発制限を行った。このため、定期便欠航が翌日のものも含めて215便、当日の30分以上の遅延便が1,462便発生し、多数の旅客に影響を与えた。

パソコンのゲームで航空管制業務を行うゲームがあり、これをやった方はすぐにおわかりいただけると思うが、現在のように航空交通量が増大している中で、三次元の空間を高速度で移動し続ける航空機の管制を行うにはコンピュータの支援が不可欠である。特に、羽田空港のように離着陸の多い空港では、システムを活用してピーク時に2分に一機の発着を行っているが、これがマニュアルになれば、離着陸可能な便数は大幅に低下する。

なお、航空管制システムの全体像については、国土交通省のホームページを参照されたい。

http://www.mlit.go.jp/koku/koku.html

### 1.3.2 航空管制システム障害の原因

国土交通省の発表によれば、今回の障害の原因は次のように説明されている。（詳細は、国土交通省のホームページhttp://www.mlit.go.jp/kisha/kisha03/12/120312_.htmlを参照のこと。）

１．ＦＤＰシステムの障害の原因調査の結果

（１）直接的な原因：プログラムミス

①2002年9月に変更したプログラム（共通のデータ処理プログラム）にミスがあったものの、その時点では問題は生じなかった。このミスは、「共通のデータ処理プログラム」が作業する対象となるデータエリアが、プログラムが格納されている区画の末尾に位置することになる場合に限り、その作業が「不正な作業」とされ、システムがダウンするもの。

②その後、2003年3月1日に変更したプログラム（防衛庁システム対応プログラム）の導入によ

りＦＤＰ内の作業の環境が変わった。すなわち、「共通のデータ処理プログラム」が作業する対象となるデータエリアが、プログラムが格納されている区画の末尾に位置することになった。
③同日７時、「オンライン統計処理プログラム」が起動し、このミスのあった「共通のデータ処理プログラム」に作業を命令したため、作業を開始したところ、「不正な作業」とされ、システムがダウンした。
④日本電気（株）（ＮＥＣ）では、社内において作業を行っていたところ、１月末、「共通のデータ処理プログラム」にミスがあることを検出したが、国土交通省に報告することはしなかった。
⑤ＮＥＣによれば、このミスがＦＤＰ内に内在した 2002 年９月以降 2003 年１月末までに、すでに問題なく運用されていたことから、このミスが致命的な問題を引き起こすとの問題意識はなく、国土交通省に対して、「防衛庁システム対応プログラム」については、改修措置を講じる旨の申し出をしなかった。
（２）事前チェックが不十分
①ＦＤＰ等に用いられるプログラムについては、航空局のシステム開発評価・危機管理センター（ＳＤＥＣＣ）において、事前チェックを行っているが、今回の「防衛庁システム対応プログラム」の変更については、問題の「オンライン統計処理プログラム」が起動する午前７時を挟んだ 24 時間稼働のチェックは行っていなかった。
②これは、「防衛庁システム対応プログラム」と今後変更を予定していたプログラム（広域レーダー対応プログラム）とを合わせて、24 時間稼働のチェックを行ったところ問題がなかったことから、「防衛庁システム対応プログラム」自体については、24 時間稼働のチェックを行わなかったものであるが、いずれにしろ、実態に即した事前チェックとは言いがたかった。
国土交通省が発表した、今回の障害原因は以上のとおりである。

### 1.3.3 航空管制システム障害の教訓

今回の障害に対して、国土交通省はシステム維持管理フェーズにおけるテストを強化して、24 時間稼働などの実運用条件に則したテストを入れる改善をただちに実施しようとしている。また、「航空交通管制情報処理システムのフェイルセーフのあり方等に関する技術検討委員会」を開催し、障害発生時に全体システムのダウンを防止するように、ソフトウェアの独立性を高める方法等について検討を進めている。今後、この委員会の検討が進むにつれ、今回の障害原因の背景についても明らかになっていくことを期待する。
情報システムのリスクマネジメントの観点から、今回の障害の教訓としては、フェイルセーフの考え方をシステムに実装する技術面に加え、システム開発／運用における管理面についても重視する必要がある。

## 1.4 ネットウイルス

2000 年以降のコンピュータウイルスはさまざまな点で故意の攻撃としての性格が強く、被害も大きくなってきている。特に注目されるのは、2003 年１月に発生したインターネットの広域の性能低下やネットワークのダウンにつながったＳＱＬスラマーワーム 事件である。以下にこの事件について紹介し、この事件から得られる問題をリスク分析の観点から分析する。

### 1.4.1　ＳＱＬスラマーワームによる事件の全貌

カリフォルニア大学サンディエゴ校の『サンディエゴ・スーパーコンピュータ・センター』、カリフォルニア大学バークレー校、シリコン・ディフェンス社（カリフォルニア州ユリーカ）、ＮＰＯ国際コンピュータ科学研究所は、共同でＷｅｂサイトで報告を発表している。報告書では、Sapphire worm（別名ＳＱＬスラマー）は 8.5 秒ごとに感染数を２倍に増やし、攻撃開始から 10 分以内に、世界中の７万 5,000 台以上のコンピュータに感染したことが述べられている。正確な数字はわかっていないが、世界中で数千～数万台のホストに感染した可能性が指摘されている。単純に計算すると、感染したホストは、合計で数十億のワームをコピーし世界中にばら撒いたことになる。短時間にこの数のワームがインターネットにばら撒かれたため、インターネットのトラフィックに重大な遅延が発生し、インターネットに頼っている多数の事業の業務に支障が出た。（http://www.sdsc.edu/Press/03/020403_SAPPHIRE.html）

このサイトでは、2001 年７月に起きた悪名高い Code Red worm が全世界のコンピュータホストに感染するのに 12 時間かかったのに対して、ＳＱＬスラマーは 10 分しかかからなかったという驚異的な拡散の速度について分析している。その理由として、このワームの本体が 376byte ときわめて小さく、感染するための転送がきわめて短く拡散しやすいこと、また、全世界のインターネットの帯域が急速に増大していること、サーバの処理能力の向上から、短時間に転送されたものと結論づけている。

### 1.4.2　被害にあったサイトと問題の本質は人災

被害にあったサイトについては、上記Ｗｅｂに「発生後 10 分で感染した地域」が報告されているが、インターネットの発展した国が多い。Code Red と比べると、ＳＱＬスラマーの問題はより深刻であった。これは、ＳＱＬスラマーがネットワークのダウンをもたらしたからである。

国別に被害状況をみると、アメリカ 43%、韓国 12%、中国６%、日本２%となっており、アメリカの被害総数は多いにもかかわらず、ネットワークのダウンが比較的軽症であった。一方、韓国は 12%であるにもかかわらず、国中のインターネットが終日ダウンして利用できなかった。

特に韓国では、表１－３に示すようにＳＱＬスラマーによって１月 25 日はインターネットがほとんど輻輳状態になり、電子メールですら送受信ができなかったと報告されている。このために、インターネットによる商取引やネットワークゲームなどを含めると４兆ウォン（約 4,000 億円）の被害が出たと報告されている。この事態はインターネットが急速に発展している中国でも同様で、国家的な問題となった（図１－１）。

表１－３．総務省が調査した韓国のＳＱＬスラマー事件の状況について（経過）

| | |
|---|---|
| １月 25 日 | インターネット障害発生（14 時頃から深夜まで） |
| １月 26 日 | 情報通信部長官が、記者会見を行い、<br>「１月 25 日のインターネット障害事故への緊急対応」及び「インターネット障害事故に当たっての国民行動計画」（ユーザがとるべきワーム対策等）を発表。 |
| １月 26～27 日 | 主要情報通信施設を点検（ＩＳＰは、25 日に 1434 ポートを遮断） |

出典：総務省ホームページ（http://www.soumu.go.jp/s-news/2003/030210_2.html#01）

26日未明の新華社電によると、中国でも25日午後4時（日本時間同5時）7分からインターネットへの接続ができなくなる大規模な障害が発生した。国家コンピューターネットワーク応急処理センターがウイルスを取り除く措置を実施し、25日同9時半（同10時半）には、ほぼ回復した。

図1－1．中国でのSQLスラマー事件

出典：日経NETニュース　2003年1月26日（http://www.nikkei.co.jp/）

一方、日本では、図1－2のように全世界からのワームが来たものの、記事にあるように大規模なネットワークのダウンには至っていない。

総務省によると、同日夜までに一部のプロバイダー（接続業者）でサービスを制限したとの報告を受けたが、大きな混乱は確認されていない。警察庁は、サイバーテロやウイルス侵入を監視する部署を中心に警戒を強めている。
（中略）
日本国内のトラブルも原因は同じとみられるが、韓国の情報が早期に伝わっており、同省は「欠陥への対処を迅速に行った業者が多かったため、大規模な混乱に発展しなかったのではないか」としている。
ネット上の東大の報告によると、東大では25日午後2時半ごろ、SQLの特定のポートに多量のデータを送り付ける未知の「ワーム」と呼ばれる不正プログラム、またはウイルスを検出したという。
情報セキュリティー会社「ラック」（東京都江東区）によると、同日午前から、常時監視している全国の企業数十社などのサーバー、送り主不明の「UDP」と呼ばれるデータが大量に送られているのを確認。午後2時半ごろからは、データが1時間に数十万件にまで急増した。

図1－2．日本でのSQLスラマー事件

出典：日経Netニュース　2003年1月25日（http://www.nikkei.co.jp）

日米では、図1－2に示すようにワームによって多数のサイトが被害を受けたにもかかわらず、ネットワークはダウンしなかった。これは、図1－3に示す総務省の調査分析に示されているように、韓国では急速にブロードバンドが広がったため、インフラが十分に整備されないままであったことがわかる。特に、ワームについては2002年7月に問題点が指摘されており、対策のパッチプログラムも提供されていたにもかかわらず、対策を打っていなかったことがわかる。また、DNSサーバなどネットワークの根幹にかかわるサーバへの対策がなされていなかったこと、このような被害を想定した二重化などの信頼性対策がなされていなかったことが問題点として挙げられる。そのため、このワームの問題点は、ワームという重大な犯罪的な問題以上に、ソフトウェアでの対策を怠ったり、不正コピーのソフトウェアを利用していたための人災としての側面が大きいことがわかる。（日本やアメリカでは、ソフトウェアの不正コピー問題やサーバなどのオペレーション問題では、中国、韓国よりも若干進んでいたため、被害が少なかったといえよう。）

○　韓国のブロードバンド普及
　韓国ではブロードバンド普及率が高く、急速にワームが拡散。
○　韓国のインターネットインフラの特徴
　韓国はインターネットの全てのポートを原則オープンに設定する傾向があり、日本と比べ、今回のワームの攻撃対象となるサーバが多かった。
○　ユーザのシステムにおけるセキュリティの脆弱性
　違法コピーの存在、正規ユーザでも運用断やコスト増への懸念等から、パッチ（修正プログラム）を当てていなかったＳＱＬサーバが多く存在。
○　日常からのセキュリティ対策の推進、ユーザのセキュリティ意識向上の必要性
　情報通信部は、民間との連携によりセキュリティ・ポータルサイトを開設する方針。
○　ＤＮＳサーバの障害
　現在、専門家による更なる技術的分析を実施中。
○　新たなワーム発生の危険性
　今回の事件により、近い将来、新たな同種のより悪性のワームが発生する危険性も想定されることから、今後とも予断を許さず対応することが必要。
○　官民の連携、国際的な連携の重要性
　ワーム等への対策には、早期検知・対応が最も重要。障害の兆候等の情報を迅速に交換しあい、被害を最小化、または未然に防ぐことのできる体制の早急な構築が必要。

図１－３．総務省が調査した韓国のＳＱＬスラマー事件の分析について
出典：総務省ホームページ（http://www.soumu.go.jp/s-news/2003/030210_2.html#01）

1.4.3　リスク分析から見た問題の本質

ＳＱＬスラマー問題からは、次の２点がリスク分析の面から重大であることがわかる。
①ワームやウイルスなどの発生は予測できない。そのため、事前対策には限界がある。また、今まで、これらの問題はサーバがダウンすることであったが、今回のようにサーバがダウンすることなく、ワームをより拡散する方向で被害の拡大が加速する可能性がある。
②ワームが拡散することで、ネットワークがダウンすることがありうること。すなわち、ワームのトラフィックが増大し、ネットワークを流れるトラフィックの大多数を占めるようになってしまい、これを止めるのは、インターネットのように自立的なシステムが接続され、中央からの制御ができない場合、問題はより深刻になり、ネットワークが使えなくなる。これに対する抜本的な解決はなく、インターネットを利用するユーザのモラルに頼らざるを得ない。
③このワームの問題の本質に、不正コピーのような隠された問題やオペレーションで対応を怠るというような問題があり、対策が明示されていても、本質的な解決になっていない。

すなわち、問題の本質はインターネットが本質的に持つ脆弱性による問題であり、これらの対策はきわめて難しい。図１－３に総務省が示しているように、官民をあげ、かつ、国際的な枠組みを構築していかなければならない。したがって、このような仕組みが発足するまでは、企業や組織にとってはリスクとして対策を考えなければならない。リスクとしては次の点が挙げられる。
①ワームによるサーバのダウン

②サーバダウンからの回復（サーバが利用できないための事業の停止、中断をどう防ぐか）
③インターネットのダウン（ネットワークが利用できないための事業の停止、中断をどう防ぐか）
④ワームをばら撒く加害者になる（図１－３に指摘されているようにトロイの木馬のようなケースでワームを仕込まれる可能性がある）

リスク対策としては、これからの課題が多いが、次の点が挙げられる。
①ワームに対する検出、削除、被害の最小化
②サーバのダウン防止およびワームの場合のサーバの迅速な停止
③ワームなどの情報のすばやい入手
④ワームに感染したときのすばやい対策(ベンダやＩＰＡなど相談できる窓口,コンサルタント、保守サービスの確保)
⑤インターネットが利用できない場合の連絡手段、事業の継続手段の確保

以上、ＳＱＬスラマーによって、新しいリスクがあることがわかった。これに対処するには、問題はきわめて難しいことがわかってきた。すなわち、今後、ワームの感染対策のみならず、サーバやネットワークがダウンして利用できない状況を考慮にいれた新しいリスクマネジメントシステムが必要になっている。

## 1.5 個人情報関連

### 1.5.1 個人情報の保護

個人情報保護法に関するニュースがしばしば話題になっている。

「個人情報保護基本法」を 2001 年の通常国会で成立させるべく作業が行われたが、いまだに成立にいたっていない。

したがって、わが国ではまだ、国として個人情報保護は法制化されておらず個人情報の保護に関する環境が十分整っているとはいえない状況にある。

個人情報保護に関する国際的な動きとしては、早くから個人情報のもつ価値に注目し、その運用に関するリスクを重視して法制化の動きを早めている国が多い。

たとえば、ＥＵでは「個人データ処理に係わる個人の保護および当該データの自由な移動に関する欧州会議および理事会の指令」（1995 年）を軸に関係各国は独自に法制化を進めている。

また、アメリカにおいては、個人情報を扱うビジネスの健全性の保障（プライバシーマーク）として、民間企業からなる非営利団体が個人情報管理を健全に行っている企業に対し、その証となるマークを付与することで個人情報保護を推進している。

日本においても、日本情報処理開発協会（ＪＩＰＤＥＣ）が 1998 年４月から個人情報管理を適切に行っている民間企業に対し、プライバシーマークを交付する制度を実施している。

個人情報保護に関する十分な対応ができていなければ、国としてはもちろんであるが、企業としても国際的な活動に支障がでるおそれがあることを考えると、プライバシーマーク制度の普及は重要な課題である。

現在までのプライバシーマーク使用許諾事業者数は表１－４のとおりである。

表１－４.プライバシーマーク使用許諾事業者数（2003年３月現在）

| 業　　種 | 使用許諾事業者数 |
|---|---|
| 情報サービス・調査業 | 315 |
| 生活関連サービス業 | 10 |
| 印刷・出版業 | 35 |
| 学習塾・教育関係業 | 21 |
| 人材紹介・派遣業 | 31 |
| その他 | 56 |
| 合　　計 | 468 |

では、なぜ個人情報を保護する必要性が高まっているのであろうか。

その理由として、主に以下の内容が考えられる。

①顧客情報をはじめとする個人情報は、企業などが営業活動を有利に展開する際の欠くことのできない有効情報として、その価値が高まっている。

②最近はＩＴ化によるインターネットのめざましい普及が、個人情報の収集を容易にしている。

③インターネット普及の他、カード・携帯電話の普及・住民基本台帳ネットワークシステムの運用開始など、社会生活がより便利になるにつれ、個人情報が不用意に他に流出されるリスクも増している。2002年度中に明るみに出た、わが国の個人情報漏洩の主な実例は後述する。

④個人情報の漏洩があった場合、情報を漏らされた個人は被害を蒙る可能性が高く、また一旦漏洩した情報は取り消すことができず、漏洩の範囲がどの程度に及ぶか計り知れない。

⑤個人情報が漏洩したことによる被害の訴訟が考えられる。

約21万人分の住民票データが流出した京都宇治市の事件では、2002年末に大阪高裁が宇治市に対し１人１万５千円の損害賠償額の判決を下したが、これを不服として宇治市は上告している。

宇治市住民基本台帳データ大量漏えい事件－京都地判
平成13年２月23日（第一審）・大阪高判平成13年12月25日（控訴審）・最決平成14年７月11日（上告審）

宇治市の住民基本台帳データ21万数千人分を外部委託業者が事務所内で保管中、持参の光磁気ディスクにアルバイト大学院生が無断でコピーして持ち出し、データを名簿業者がウェブで販売した事案で、プライバシー権侵害に基づき住民に対する損害賠償責任を市に認めた。

### 1.5.2　個人情報に関する実態調査

ＪＩＰＤＥＣが行った「わが国における情報セキュリティの実態－情報セキュリティに関する調査集計結果」（2002年３月）によると、個人情報保護について次のような結果がでている。
（http://www.jipdec.jp/security/01sec.html）

Q個人情報の利用目的はなんですか？（複数回答）

| | | |
|---|---|---|
| 1 | 売買等契約の履行 | 18.0% |
| 2 | 顧客サポート | 38.3 |
| 3 | 代金等の回収 | 19.5 |
| 4 | 情報提供 | 22.3 |
| 5 | マーケティング | 25.6 |
| 6 | 商品開発 | 7.8 |
| 7 | 従業員の管理（インハウス情報） | 57.1 |
| 8 | 行政サービスの履行 | 9.5 |
| 9 | その他 | 3.9 |
| 無回答 | | 10.3 |

個人情報の利用については「従業員の管理」がもっとも多く、次いで「顧客サポート」、「マーケティング」の順になっている。

従業員に係わる情報を個人情報とみなしてみれば、従業員管理での利用は 100%になるはずであるが、約 40%の事業体は必ずしも従業員情報が個人情報であるとの認識がないことがわかる。

個人情報については、次のように定義されているのが一般的である。

「個人情報」の定義
個人に関する情報であって特定の個人を識別できるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む）。

Q利用している個人情報の収集方法はどのように行っていますか？（複数回答）

| | | |
|---|---|---|
| 1 | 申込書等によって情報主体（当該個人）から直接収集 | 76.7% |
| 2 | 各名簿業者等から購入 | 2.2 |
| 3 | グループ企業から入手 | 4.3 |
| 4 | 他社から提供を受ける | 3.8 |
| 5 | 業務委託契約等に基づき提供を受ける | 12.5 |
| 6 | その他 | 7.2 |
| 無回答 | | 12.4 |

「情報主体から直接収集」が最も多く、次に多いのは「業務委託契約等による提供」である。

Q情報主体から直接に収集する場合、収集・利用目的について同意を取っていますか？

| | | |
|---|---|---|
| 1 | はい | 59.1% |
| 2 | いいえ | 21.6 |
| 無回答 | | 19.4 |

個人情報の収集に関しては、約60%が同意を取っているが、「取っていない」が約20%を占めている。本人の同意を得ずに個人情報を収集・利用していることは問題と考えられる。

Q間接的に収集する場合、収集・利用目的について情報主体から同意を取っていますか？

| | | |
|---|---|---|
| 1 | 情報主体から同意を取っている | 17.4% |
| 2 | 入手先が情報主体の同意を取っていることを確認している | 18.5 |
| 3 | 何もしていない | 27.4 |
| 無回答 | | 36.6 |

「何もしていない」が27.4%と多いのは問題である。
情報主体の関知しないところで情報が一人歩きしている危険がある。

Q貴事業体では顧客等の個人データをコンピュータ処理する際に、個人情報保護の観点からの内部規程（たとえば、個人情報保護規程など）を定めていますか？

| | | |
|---|---|---|
| 1 | 定めている | 25.2% |
| 2 | 作成中である | 6.1 |
| 3 | 検討中である | 16.2 |
| 4 | 定めていない | 40.4 |
| 無回答 | | 12.1 |

コンピュータ処理上での個人情報の取扱いに関しては、約30%が内部規程により管理している。
しかし、「定めていない」、「検討中である」を合わせると、56.6%が何の規制も設けていないのは問題である。

Q個人情報の廃棄方法を個人情報保護規程に定めていますか？

| | | |
|---|---|---|
| 1 | 定めている | 64.9% |
| 2 | 作成中である | 14.7 |
| 3 | 検討中である | 6.7 |
| 4 | 定めていない | 8.9 |
| 無回答 | | 4.9 |

「検討中である」、「定めていない」を合わせると約15%となるが、これは無視できない問題である。

Q個人情報の取扱いに関する責任と権限を持った管理者を定めていますか？

| | | |
|---|---|---|
| 1 | 定めている | 33.8% |
| 2 | 作成中である | 17.3 |
| 3 | 定めていない | 37.0 |
| 無回答 | | 11.8 |

個人情報の取扱いに関して管理者を「定めている」よりも「定めていない」の方が若干多い結果となっている。

個人情報保護の取扱いについてはまだ不明瞭な点が多い証拠である。

Q個人情報の取扱いに関する情報主体からの苦情処理を行う窓口がありますか？

| | | |
|---|---|---|
| 1 | ある | 39.3% |
| 2 | ない | 48.2 |
| 無回答 | | 12.5 |

苦情処理窓口は非常に重要な機能であるが、48.2%は窓口を設置していない。

Q情報主体から、自己情報の開示や訂正または削除等を求められた場合、応じることになっていますか？

| | | |
|---|---|---|
| 1 | なっている | 50.3% |
| 2 | なっていない | 31.1 |
| 無回答 | | 18.7 |

情報主体からの自己情報の開示、削除等の要求への対応については、「なっていない」が31.1%であり、個人情報の取扱いはきわめて慎重を要するが、依頼に応じないということは問題である。

Q個人情報を外部委託する場合に交わす条項には何がありますか？（複数回答）

| | | |
|---|---|---|
| 1 | 秘密保持義務 | 41.4% |
| 2 | 責任分担 | 10.7 |
| 3 | 個人情報の適正な管理 | 24.7 |
| 4 | その他 | 1.5 |
| 5 | 外部委託を行っていない | 42.2 |
| 無回答 | | 13.9 |

「秘密保持義務」と「個人情報の適正な管理」を合わせると、66.1%になる。

これらを考えると、個人情報の外部委託については十分な配慮がなされていると考えられる。

Q（財）日本情報処理開発協会の「プライバシーマーク制度」（平成10年4月運用開始）を知っていますか？（複数回答）

| | | |
|---|---|---|
| 1 | 知っている | 40.4% |
| 2 | 知らない | 49.0 |
| 3 | プライバシーマークを利用したい | 3.3 |
| 4 | 利用したいと思わない | 0.8 |
| 無回答 | | 8.5 |

ＪＩＰＤＥＣが運用している「プライバシーマーク制度」を「知っている」は約40％であった。個人情報保護に対する公的取組み自体に対する周知度はまだあまり高くない。

以上個人情報保護の実態調査からみると、まだまだ十分とはいえない面が多々ある。

ＩＴ化などによる社会生活の利便性を高めることは大切であるが、同時に、個人情報漏洩のリスク対応を十分考慮することも忘れてはいけない。

### 1.5.3　個人情報の漏洩

個人情報漏洩を原因別に整理してみると、悪意によらないものと、悪意によるものとに分類することができる。

悪意によらない個人情報の漏洩としてはさらに「うっかりミス」によるものと、「個人情報保護についての関心の低さ（認識の甘さ）」によるものとに分けられる。

悪意による個人情報の漏洩はさらに「金銭目的によるもの」と「個人情報を不正に利用する目的によるもの」とに分けられる。

１．悪意によらないもの

（１）うっかりミスによるもの

・プログラム上のミスにより、個人情報流出のおそれで首相官邸ホームページが一時閉鎖された。
・インターネットによる総務省の「電子申請・届出システム」に欠陥があり、個人情報流出のおそれがあった。
・少年刑務所で、男子受刑者の個人情報が書かれている少年簿を紛失した。
・カード入会申込書等を封入した本支店間の配送袋が配送中に所在不明となった。
・市のホームページで非公開とすべき個人情報を公開してしまったため、美術館入館者などの個人情報が閲覧可能な状態となっていた。
・県立工業高校で今春卒業した卒業生の実名、連絡先等が個人のホームページに掲載されていた。
・県のホームページで情報公開請求者の氏名を完全に削除しなかったため、パソコンの操作次第でホームページに表示される状態となっていた。
・信販会社がクレジットカード利用の請求書に他人の銀行口座番号を誤印刷した。
・インターネットで電話回線の新設を申し込んだ契約者に送信していた契約確認メールが、誤って無関係の利用者にも送信されていた。
・新聞社が自社サイトで解説している掲示板で、キーワード検索を行うと個人情報の一部が表示されるバグが存在していた。
・シューズ販売サイトを利用した顧客の個人情報がシステムのミスにより、インターネット上で流出した。
・結婚相手探しの男女の顔写真がシステムのミスにより、インターネット上で多数流出した。
・本来非公開であるはずの薬学生の個人情報が外部から閲覧できるようになっていた。
・老舗菓子販売店の通信販売の顧客情報と思われる顧客情報が、インターネット上で流出した。
・インターネット接続の契約者にメールを一括送信する際、誤って契約者全員のアドレスが表示される方法でメールを送信していた。

・ウイルス駆除ソフトの利用者がユーザ登録を更新する際、他人の名前やメールアドレスが誤って表示された。
・県の報道資料で、来日運動選手のパスポート番号等の個人情報を誤って掲載したまま配布した。
・携帯電話の請求書に、他人の請求内容および通話明細を誤って封入し送付した。
・登録されている全学生の顔写真が学内コンピュータシステムから認証なしで閲覧可能な状態であった。
・旅行宿泊先予約サービスでプログラム上の不備により、同サービスを利用した他の顧客の予約情報が表示される場合があった。
・高速道路の料金未納者リストが管理ミスにより外部に流出した。
・国民健康保険税の口座振替領収証書で、金融機関名や口座番号などの個人情報がシール張り忘れの状態で送付された。
・市立中学校で、生徒の小学校時代の病歴などが記録されている「児童生徒健康診断書」と成績表などが記録されている「指導要録の抄本」が紛失していた。

（2）個人情報保護についての関心の低さ（認識の甘さ）によるもの
・大学で教授のホームページに学生の試験結果や評価などを実名入りで掲載し、公開していた。
・原子力発電所の周辺地域住民に給付される、原子力立地給付金の受け取りを拒否した人のリストを電力会社から受け取り、立地自治体に提供していた。
・某府議会で問題教員を取り上げた質疑をめぐり、関連する児童の実名を府議会のホームページに掲載していた。
・アンケートに苦情や意見を書いた人の住所・氏名をリストとしてまとめ、市庁舎内で回覧していた。
・県営アパートの家賃を１年分以上滞納している入居者リストをメモ用紙として使用していた。
・某省庁で情報開示請求者の身元別一覧表やグラフを含んだ資料を作成し、幹部らを対象とした講習会で配布していた。
・市税に関して個人情報が印字してある内部文書を持ち出して、裏面をメモ用紙として利用し、町内会で配布していた。
・農地の転用手続きに関する文書の情報公開を県に求めていた人の名前を書いた資料を作成し、農業委員に配布していた。
・電話相談の内容の一部を相談者に無断でテープに録音し、カウンセラー養成講座の教材に長年使用していた。
・大学受験希望者の個人情報が１年以上にわたってインターネットで容易に閲覧可能な状態にあった。
・簡易保険の契約者情報が記載されているリストを来客用のメモ用紙として使用していた。
・人材派遣のＷｅｂサイト上にある個人情報を含むファイルが、外部から閲覧可能であった。

２．悪意によるもの
（１）金銭目的によるもの
・巡査部長が、捜査と偽って県内の陸運事務所から車の所有者に関する情報を入手して知人の自

動車販売業者に漏らし、謝礼として２万円を受け取っていた。
・郵便預金の口座番号や残高情報を漏洩したとして、郵便局員と調査事務所経営者を逮捕、見返りとして現金の授受があったものとして追求している。
・警察ＯＢが経営するコンサルタント会社に、軽四輪自動車の車籍紹介で得た個人情報を漏らしたとして、警察官ら３人を逮捕、現金授受の有無について追及している。

（２）個人情報を不正に利用する目的によるもの（金銭目的か否か明確でないものも含む）
・小学校３校で保健室に保管してあった児童全員の発育記録が盗難にあった。
・市役所の複数のパソコンがウイルスに感染、個人情報など重要情報が外部に流出した可能性もある。
・エステ大手のホームページから個人情報が流出したが、不正アクセスの可能性が高い。
・建材メーカのホームページから個人情報が流出したが、不正アクセスの可能性が高い。
・エステ大手のホームページから不正アクセスにより個人情報が流出したが、他にも大学や企業などで同様の流出があったことが判明した。
・放送関連会社のホームページから、不正アクセスによりセキュリティプログラムを消去して視聴者個人情報を流出させた。
・インターネット事業を展開している会社が運営する女性向けホームページで、ネット懸賞に応募した個人データが悪質なハッキングにより流出した。
・市の住民情報オンラインシステムを使い、個人の納税記録などが役所内で不正に照会されていた可能性があることが判明した。
・菓子メーカがインターネットのサーバ上で保管していた顧客の個人情報などが、外部から不正にアクセスされ流出していた。
・パソコン教室を全国展開している会社のホームページから、同社に就職を希望したり、問い合わせしたりした学生や社会人の個人情報がデータ保管場所のハッキングにより流出した。
・「個人情報」を記録したパソコンが車上荒らしに遭い盗まれた。
・市のマルチメディアセンタを通して市民に提供しているインターネット接続サービスの、登録者のメールアドレスなどの個人情報が入っているパソコン１台が盗難にあった。
・関東地方などの六県で、税務署員を装い、個人情報を聞き出そうとする不審な電話が多発していた。
・開校を予定する生涯学習大学の受講申込者の個人情報を、何者かが庁内のパソコンから故意に電子メールで送信した可能性がある。
・地方自治体や小学校のコンピュータに何者かが侵入し、児童や保護者の個人情報を流出させた可能性がある。
・証券会社の顧客データが、社外の名簿業者に持ち込まれていた。
・国税局のホームページに寄せられた税務行政に関する意見や要望の一部が外部から何者かに閲覧されていたが、閲覧されていた情報の一部には住所・氏名等の個人情報が書き込まれていた。
・住民基本台帳ネットワークシステム（住基ネット）に登録されている全町民の個人情報を収めたマイクロテープが、車上荒らしに遭い盗まれた。

個人情報漏洩は、今後ますます増加の傾向にあるが、「悪意による」、「よらない」の両者とも主たる原因は、企業の内部で情報を取り扱う要員（内部、外部）が関係しているケースが多く、身近なところで情報が漏洩している。

関係者の更なる自覚と奮起が必要である。

## 1.6 内部告発

### 1.6.1 情報システムのリスクマネジメントと内部告発

内部告発は、経営に与えるインパクトとしては非常に大きなものになる。内部告発は、告発された内容そのものも問題であるが、内部告発に至るのは何らかの不適切な経営がそのこにあるとみなされることで、信用の失墜に結びつきやすい。それにもかかわらず、情報システムのリスクマネジメントを検討する場合、内部告発にかかわるリスクはあまり検討されてこなかった傾向があるように思われる。

内部告発の対象となる行為は次の３種類に分類できる。

（１）違法行為

法規に反する行為であり、刑事罰、行政罰の対象になりうる。また、違法行為の結果として、損害賠償請求や重大な信用失墜につながることが考えられる。

違法行為の例：

・ソフトウェアの知的財産権の侵害により著作権法に違反する場合

（２）権限逸脱行為

契約等で定められた権限、権利を超えた行為を行った場合には、権利の保持者によって損害賠償請求を起こされる場合がある。そのような権限逸脱行為により、信用の失墜を引き起こされることが考えられる。

・契約の範囲を超えたソフトウェア、サービスの使用
・ビジネスモデル特許など他の組織の特許への抵触
・取引先等の営業機密の漏洩
・個人情報の漏洩

（３）ポリシーに反する行為

違法でも、契約に反する行為ではないが、企業の掲げるポリシーや倫理的な問題への抵触により、信用を失墜することが考えられる。たとえ、刑事罰や損害賠償が請求されなかったとしても、信用失墜による事業への影響は無視できない。

表１－５．内部告発の対象およびその影響

<table>
<tr><td>内部告発の対象</td><td colspan="3">内部告発から予想される影響</td></tr>
<tr><td>違法行為</td><td>刑事罰、行政罰</td><td rowspan="2">損害賠償</td><td rowspan="3">信用の失墜</td></tr>
<tr><td>権限逸脱行為</td><td></td></tr>
<tr><td>ポリシーに反する行為</td><td></td><td></td></tr>
</table>

1.6.2　内部告発リスクの例

内部告発は情報システムにかかわるリスクのうち、特に経営に関するリスクと考えることができる。経営に与えるインパクトを鑑みて洗い出したリスクの例は表１－６のとおりである。

表１－６．経営に係わるリスク

| | |
|---|---|
| 製品トラブル | 製品瑕疵、製造物責任、リコール・欠陥製品、苦情処理対応トラブル |
| 知的財産権侵害 | 特許紛争、実用新案侵害、商標権侵害、著作権侵害 |
| 環境問題 | 環境規制強化、環境賠償責任・環境規則違反、環境汚染・油濁事故、廃棄物処理・リサイクル |
| 雇用トラブル | 差別、使用者責任、セクシャルハラスメント、労働争議・ストライキ・デモ、伝染病、役員・スタッフの不正・不法行為、職場暴力、集団離職、外国人不法就労、海外従業員の雇用調整、海外駐在員の安全、従業員の高齢化 |
| 法務上のトラブル | 商法違反・カルテル、独禁法違反、役員賠償責任、インサイダー取引、プライバシー侵害 |
| 資産運用トラブル | デリバティブ失敗、不良債権・貸し倒れ |
| 信用トラブル | 情報管理の不備・顧客情報漏洩、不正取引・詐欺 |
| 経営全般トラブル | 企業倫理、取引先倒産、格付下落・金融支援の停止、経営者の死亡、乱脈経営、不適切な宣伝・広告、不測事態発生時の対応 |
| 社内不正 | 共謀犯罪、役員のスキャンダル、経営者・従業員の不正・犯罪、共謀情報漏れ |

これらの問題は、直接的／間接的に内部告発に結びつく可能性がある。

1.6.3　内部告発リスクへの対策

内部告発に関するリスクを低減するには、

（１）告発の対象となるような問題の発生を低減する、

（２）内部告発となる前に、自ら適切な処置を行う、

という２点が重要となる。

（１）に関しては、コンプライアンス体制を整備し、教育の実施により内部告発の対象となるような問題を起こさない、発生したとしても早期に是正できるようにすることである。（２）に関しては、ホットラインなど問題点を早期に吸い上げる仕組みを組織体内部に整備するとともに、内部/外部監査によって適宜チェックすることが必要となる。

## 1.7　リスク情報の開示

コーポレートガバナンスの強化および株主保護の観点から、企業にリスク情報の開示を求める動きが強まっている。日本においても 2002 年 12 月 16 日の新聞紙上で金融庁が「2004 年３月期から上場企業が開示すべき情報を大幅に拡充する」方針が報道され（出典：日本経済新聞、2002 年 12 月 16 日）、その開示すべき情報の中にリスク情報が明示された。以下リスクマネジメントの重要な要素であるリスク情報をいかにステークホルダーの間で共有するかについて、最近の世界の動き、現状についてまとめる。

### 1.7.1　欧米のコーポレートガバナンスの強化

アメリカでは1970年代のウォーターゲート事件に伴う企業への調査を行った際、多くの企業が不正献金を行っていたことがあきらかになり、企業の内部統制が見直され、1992年ＣＯＳＯにより「内部統制の統合的枠組み（Internal Control-Integrated Framework)」が発表された。

また、欧州では1980年代後半から1990年代初めにかけて多くの不正取引事件や会社経営者の横領などが発生し、経営者をいかに監視するかという意味でコーポレートガバナンスの強化が検討されることとなった。これに伴いＯＥＣＤがコーポレートガバナンス原則を公表した。また、ＢＩＳも金融機関の検査基準を定めた。

### 1.7.2　ＯＥＣＤのコーポレートガバナンス

ＯＥＣＤはコーポレートガバナンスを企業を統制し指揮するシステムとして定義している。このコーポレートガバナンスの原則として、次の５項目を提案している。

①株主の権利

コーポレートガバナンスの枠組みは株主の権利を保護する。

②株主の平等性

コーポレートガバナンスの枠組みは全株主が平等に扱われるものを保証する。

③ステークホルダーの役割

コーポレートガバナンスの枠組みは、ステークホルダーと企業の積極的な協力により企業価値や雇用の創造と健全な財政の維持を促す。

④情報開示と透明性

コーポレートガバナンスの枠組みは、株式会社の財務、業績、所有状況やガバナンスを含むすべての重要事項の正確な情報開示を保証する。

⑤取締役会の責任

コーポレートガバナンスの枠組みは、取締役会による会社の戦略的指導や経営監視とともに、会社や株主に対する説明責任が確保される。

### 1.7.3　ＯＥＣＤのコーポレートガバナンスの中のリスク情報の開示

ＯＥＣＤのコーポレートガバナンスの第４項目には情報開示が定められている。ここでは開示すべき７つの項目を挙げている。

①会社の財務および業務の成果

②会社の目的

③主要な株主所有権と議決権関連事項

④取締役会構成要員と執行役員およびその報酬

⑤重要な予測しうるリスク要因

⑥従業員や他のステークホルダーに関する重要事項

⑦ガバナンスの構造と方針

この中で「重要な予測しうるリスク要因」が定められており、さらに具体例として「個別の産業や地理上の固有なリスク、事業の価格変動の大きな市場商品への依存度、金利・通貨リスクを

含むデリバティブ、簿外取引に関連するリスク、環境責任に関するリスクなど」を列挙している。環境に係わるリスクを掲げているのはいかにも欧州的と考えられるが、これ以外に事業遂行全般に係わるリスクが対象になっている。

なお、開示の範囲は株主や投資家にとり必要性のない詳細情報の開示は対象としていない。一方、リスク監視の仕組み（マネジメントシステム）を適切に設けているかという取り組み状況に関する情報開示は有益であるとしている。

### 1.7.4 ＣＯＳＯのリスクマネジメントの重視

1992年にＣＯＳＯが公開した「内部統制の統合的枠組み」の中で内部統制に主要な５つの要素を定めている。

①統制環境（Control Environment）

役職員の能力、誠実性、倫理観、経営者の哲学、権限と責任、従業員の教育、企業文化などを定める。

②リスク評価（Risk Assessment）

事業目的を達成するために関連するリスクを認識し分析し、管理方法を決定する基礎情報を提供する。事業活動の状況に関連したリスクの識別と対処の仕組みの構築が必要である。

③統制活動（Control Activities）

経営者の命令が実行されることが確実となる方針と手続き。統制活動は全指揮階層および全経営職能で行われる。

④情報と伝達（Information and Communication）

役職員各自の情報が識別認識され、上下双方向および組織間で伝達される。

⑤監視活動（Monitoring）

内部統制システムの質を継続的に評価する。その欠陥は最高経営者と取締役会に報告される。このような５つの要素のうちの第２項目にリスク評価が明確に定められている。

### 1.7.5 ロンドン証券取引所のリスク情報開示

最近のリスク情報の開示に関する方向性に重要な影響を与えたのが、1999年12月23日から適用されたロンドン上場企業に対するリスク情報の開示の義務づけである。

これは1998年６月に公にされた「コンバインドコード（Combined Code）」およびターンブル報告書「(Turnbull Report)」によっている。イギリスでは1990年代後半から企業の不祥事を防ぐために政府、ロンドン証券取引所、イングランドウエールス会計士協会において委員会が設置され、コーポレートガバナンスや情報公開について株式会社がいかにあるべきかが議論され、報告書にまとめられた。

ターンブル報告書ではリスクを事業目的達成に対する阻害要因と位置づけ、リスクの探知と内容の評価を行い、組織の人と物を用いて、リスクへの対処を決定し、実行することを求めている。そしてリスク低減に向けた行動の実効性があるか否かについて監視し、次の行動計画策定の基礎とする、この一連のプロセスとして内部統制を位置づけている。

ターンブル報告書の目次

1．導入
　・コンバインドコードの内部統制要求項目
　・ガイダンスの目的
　・内部統制とリスクマネジメントの重要性
　・グループ会社
　・追記
2．健全な内部統制システムの維持
　・義務
　・健全な内部統制システムの要素
3．内部統制の有効性の見直し
　・義務
　・有効性見直しのプロセス
4．内部統制に関する取締役会の声明
5．内部監査
6．追記
　・企業リスクおよび統制プロセスの有効性評価

ここでリスクマネジメントこそが株主資本・企業資産を守るための鍵となること、また事業環境は常に変化しており、完全で系統だった自社の取り巻くリスクの性質と程度を評価することによって会社が成立するとしている。また、リスクは合理的水準までのリスクの防止が目的であり、撲滅することが目的ではないことを明記しており、リスクを経営者としてテイクすることが利益の源泉であることも明示している。

コンバインドコードの規定により取締役会は内部統制の実効性の見直しを定期的に行い、年次報告において結果を株主に報告しなくてはならない。この情報開示規定によりリスクマネジメントが経営者の関与することになったとされている。

（参考資料［TRCEYE　Vol22．企業経営に対するリスクマネジメントの要請」東京海上リスクコンサルティング）

1.7.6　その他の国の取り組み状況

ドイツでは1998年に企業の監査および透明性に関する法律が立法化され、会社の経営の中にマネジメントシステムを導入し、財務報告書で企業が直面するリスクに対する評価を載せることとなった。

オーストラリアではシドニー証券取引所で 1995 年からアニュアルレポートにコーポレートガバナンスの活動報告を掲載する規則を定めた。この中でビジネスリスクを評価し、経営としてマネジメントを実践していること、リスクマネジメントとしてリスクの確認分析評価優先順位づけ、対処監視をすることとしている。

アメリカでは1994年にアメリカ公認会計士協会でジェンキンス報告を出し、リスクと機会の報告を改善し、リスクと機会の現状、利益に与える影響、経営者が検討したリスクと機会に関する内容を業務報告に含めるようにした。

### 1.7.7　日本のリスク情報開示の制度

金融庁では首相の諮問機関である金融審議会において、2002年12月の総会で「証券市場の改革促進」、「公認会計士制度の充実・強化」についての報告が行われ、リスク情報開示の充実が検討されている。また、旧大蔵省から金融庁へ移管された企業会計審議会においては、1999年10月の総会において、「監査基準等の一層の充実」を審議事項とすることを決定した。同審議会第二部会において審議が行われ、2002年１月の総会で「監査基準の改定に関する意見書」を公表している。政府は、2002年６月の閣議決定「経済財政運営と構造改革に関する基本方針2002」において、「預貯金中心の貯蓄優遇から株式・投信などへの投資優遇への金融のあり方の転換を踏まえた直接金融への信頼向上のためのインフラ整備など、証券市場の構造改革を一層促進していく」こととした。これを踏まえて、金融庁が2002年８月に「証券市場の改革促進プログラム」を公表、金融審議会では、同プログラムに盛り込まれた制度改定を伴う事項について、第一部会および公認会計士制度部会において具体的な議論を行い、2002年12月の総会において以下のような報告を行っている。

◇第一部会報告

①「市場仲介者に関する制度整備」、②「ディスクロージャーに関する制度整備」、③「取引所に関する制度整備」等からなる「証券市場の改革促進」についての報告を行った。このうち②「ディスクロージャーに関する制度整備」の中では、現在、有価証券報告書等で開示されている情報に加え、国際的にもその強化が求められているコーポレートガバナンスに関する「ガバナンス情報」（内部統制システム、リスク管理体制、役員報酬等）、「リスク情報」（特定取引先への依存、重要な訴訟事件の発生等）および「経営者による財務・経営分析（ＭＤ＆Ａ）」（経営成績に重要な影響を与える要因についての分析等）についての開示を充実すべきとの結論に達している。

◇公認会計士制度部会報告

①「公認会計士監査の意義とあり方」、②「コーポレート・ガバナンスと監査」、③「監査法人の独立性の強化」、④「公認会計士の資質の向上と公認会計士試験制度のあり方」、⑤「監査法人のあり方」、⑥「監視・監督の充実強化」等からなる「公認会計士監査制度の充実・強化」についての報告を行った。このうち、②「コーポレート・ガバナンスと監査」の中では、コーポレートガバナンスの充実・強化は、財務情報などの作成過程の健全性の確保、経営者の行動や内部統制システムの実効性に対するモニタリング、市場における財務情報の信頼性の向上などに大きく寄与するものであるとの考え方がなされ、企業自身の取り組みを求めるとともに、監査人についても、被監査企業のコーポレートガバナンスの重要な担い手と位置づけ、コーポレートガバナンスの充実・強化という観点からも、監査人がその使命と職責を果たすことが求められていると述べている。

出典：金融庁ホームページ（2002年12月16日ディスクロージャー・ワーキンググループ報告より）
（http://www.fsa.go.jp/singi/singi_kinyu/siryou/kinyu/dai1/f-20021216_sir/03.pdf）

本意見書では、国際的な動向も踏まえ、監査基準の全面的な改訂を行った。(2003年３月決算期から適用)

改訂のポイントとしては、①「不正発見の姿勢の強化」、②「継続企業（ゴーイング・コンサーン）の前提への対処」、③「リスク・アプローチの徹底」、④「新たな会計基準等への対応」、⑤「監査報告書の充実」の５つであるが、②「継続企業（ゴーイング・コンサーン）への対処」の中で、新たに財務諸表への「注記」を要する事象を規定している。

これによれば、経営者は企業に存続の危機がある場合、当該事象等の内容、危機の存在、当該事象等に対する経営者の対応および経営計画、当該事象等の影響を財務諸表に反映しているか否かについて財務諸表に注記しなくてはならない。監査人はそのような事象等の存在を検討し、必要な事項が適切に注記されているか否かを検討したうえで、財務諸表が適正かどうかの意見を表明しなくてはならない。

出典：金融庁ホームページ第８回金融審議会金融分科会第一部会資料他、2002年12月16日）
（http://www.fsa.go.jp/news/news.html）

この結果、2004年３月期から有価証券報告書に報告する情報を大幅に増加させ、開示水準をアメリカ並みにすることとされた。主な開示項目は取締役報酬、経営者による事業分析、リスク情報、経営者による正確性の証明などがある。

企業としては重要リスクを常に把握し、適時対処する体制の構築が求められることになる。

1.7.8　リスク情報の開示の事例

どのようなリスク情報が開示されているかについて、いくつかの事例を述べる。なお、リスク情報の開示については

①リスクそのものの評価

②リスクマネジメントや内部統制の体制

の二つが含まれている。

・A社

景気リスク、為替リスク、制度リスク（会計基準の変更）、価格リスク、（株価変動）、人材リスク、戦略リスク、知的財産侵害リスク、マーケティングリスク、製品品質、製造物賠償責任リスク、情報システムの災害、停電などによる損害発生のリスク、政府規制のリスク、海外事業展開によるリスク、従業員への給符債務リスクなど

・B社

ビジネスリスク、オペレーショナルリスク、供給リスク、財務リスク、人的資源リスク

・C社

リスクマネジメントの基本姿勢、リスクマネジメントの手法、リスクマネジメント委員会、マーケットリスク、為替リスク、利率変動リスク、信用リスク

・D社

内部管理体制、リスク管理体制、検査体制、総合リスク、信用リスク、市場リスク、事務リスク、システムリスク、法務リスク

・ナスダックジャパンが例示した投資家が確認すべきリスク情報（出典：日本経済新聞、2000年5月21日）

◎企業内部要因によるリスク

・事業の歴史、利益がマイナスである、業績が一部の人物に依存、増資・追加資金の必要性、特許・技術・著作権、業績の著しい変動、新製品開発に関する情報、製品サービスの集中、事業の拡大縮小、役員の免責、損害賠償保証

◎企業の外部要因によるリスク

・政府などの許認可、競合相手、特定取引先への依存、損害保険加入有無、消費者の嗜好動向、販売地域の地理的要因、業界固有の問題、訴訟問題

◎その他のリスク

・税制変更による影響度、製造量の限界、在庫リスク、倒産リスク、海外営業による為替変動リスク、一般的経済要因の影響、配達コスト、金利への感応度

◎コーポレートガバナンス

・配当、株価、公募資金の使途

・金融検査マニュアルのリスク

金融検査マニュアルでは金融機関に対し、次のリスクを明示して対処することを求めている。

①市場リスク
②流動性リスク
③信用リスク
④事務リスク
⑤システムリスク

これに対応し、都市銀行ではアニュアルレポートにそのリスクの状況につき開示を行っている。

ある銀行のアニュアルレポートからシステムリスクについて開示情報を要約すると、次の事項が開示されている。

『システムリスクとは「コンピュータシステムの停止や誤作動、不正利用により被る企業のリスク」と定義づけている。対策として、セキュリティポリシーをはじめとする諸規定、諸基準を定めている。金融庁の「金融検査マニュアル」、（財）金融情報システムセンター（ＦＩＳＣ）の「安全対策基準」を参考にリスク評価を実施し、安全対策をそのリスクに基づき実施している。

大きなリスクとして障害をあげている。この障害対策としてシステムインフラの二重化、東西２センタによる災害対策システムの設置を実施している。またお客様のプライバシー保護、情報漏洩の防止のための情報の暗号化、不正アクセス排除対策を実施している。

コンティンジェンシプランの作成と必要に応じた教育訓練の実施を行っている。』

1.7.9　リスク情報開示と情報システムリスク

前章の事例の中で各社ともさまざまなリスクを重要視し、その対応について開示している。その中ではＡ社と銀行がシステムリスクについて取り上げている。

リスクマネジメントではまず企業が企業を取り巻くリスクを洗い出し、その中で企業の経営に

大きなものから優先順位をつけて対応していくことが求められる。したがって情報システムへの対応も、情報システム部門に係わっている人間にとっては重要なリスクであるが、企業経営全体にとってどの位置づけにあるのかを把握し、リスクに応じた対応を求めることが必要である。リスクを過小評価して情報セキュリティへの経営資源の配分が不足することが問題であることは当然であるが、リスクが小さいにも係わらず、やみくもに情報セキュリティに予防予算を投入することも避ける必要がある。

そのためＪＲＭＳでは情報セキュリティ対策を求める前に経営としてのリスク評価を実施し、その企業の中での情報システムリスクの位置づけを認識してからその対応策の実施状況を評価することとした。

ただし、一般的にいってリスク情報の開示の対象に至らない二番手グループのリスクであってもリスク対応は必要であり、開示しなかったからといって、まったく対応しなくてよいということではない。

# 2．情報セキュリティに関する最近の動向

## 2.1　情報環境の変化

いまやコンピュータウイルスやハッキングを狙うポートスキャンは日常茶飯事となっており、情報セキュリティが経営者にとっても聞きなれない言葉ではなくなってきた。このような人為的なリスクが情報システムのリスクであるのはとても残念なことであるが、一方企業の中で情報システムが中枢に入り、いまや情報システムがなければ企業や自治体の活動が不可能となったことも事実である。特にこの２～３年で大きく変わったのは、多くの企業で一人に１台に近いほど端末機が行き渡ったこと、また電子メールでの企業間情報交換が基盤となったこと、そして多くの企業がホームページを立ち上げ、Ｗｅｂを通じて情報入手することが普及したことである。

いったん実現してしまうとずっと前からこのような事業環境であったと思いがちであるが、世界を揺るがした 2000 年問題（以下、「Ｙ２Ｋ問題」という。）に対応していた 1999 年当時では、まだ中央官庁や多くの自治体では各部門にホームページが検索でき、電子メールが可能な端末が最低１台程度設置されていた状況であった。また 1999 年後半になって各企業がホームページにＹ２Ｋに関する自社の対応や製品に関する情報を公開し、また他社の情報をホームページで確認することが行われ始めたところであった。官庁や企業の情報交換もテキストベースや添付ファイルの取り扱いなど慣れていなかったことなど、隔世の感がある。Ｙ２Ｋ問題の解決にはインターネットを用いたメールとホームページによる情報交換が大きな役割を果たしたと考えられるが、情報システム環境の進歩という観点からも、このＹ２Ｋ問題対応を通じてメールとホームページによる情報交換の利便性に経営幹部が気がつき、その後のＩＴ化の促進に寄与したと考えられる。

さらにこのメールとホームページ検索の利便性は各個人の自宅にもパソコンが導入される契機となり、いまや各家庭には複数台数のパソコンが存在し、メール交換やホームページ検索による情報収集、また個人のホームページ作成などが普及してきた。したがって、企業の情報開示もいまや記者会見やニュースリリースと同様にホームページでの情報開示が当然となっており、情報システムは今までの社内製造事務部門の効率化の中心的な存在である基幹システムなどに加えて、情報の共有化の基盤としてのメールやホームページの重要性が高まってきている。ここにきてこれらの情報システム環境の社会基盤の充実を踏まえて、電子自治体の構想や電子商取引が実現されようとしている。

## 2.2　ＩＳＭＳ制度の発展

情報システムは 1960 年代、1970 年代に会計や経理などの効率化など、主に基幹システムの構築から企業の中枢に取り入れられてきた。情報セキュリティの必要性とそのあり方については情報システムがきわめて高価な特殊な機械であるといった時代から議論されてきた。その後情報通信技術の発展により、一握りの技術者だけが関与する世界から、誰でもがパソコンを手にするのが当たり前の時代に変化したことに伴い、情報セキュリティの考え方も変化してきた。

日本のみならず各国でも情報セキュリティのあり方が議論されてきたが、その中で 1993 年英国で「Code of Best Practice, Information Security Management」が作成された。これが 1995

年に英国の国家規格「BS7799;1995　A Code of Practice, For Information　Security Management」となった。この「BS7799」はパート１が情報セキュリティ管理実施基準、パート２が情報セキュリティシステム仕様となっており、このうちパート１が2000年９月に国際規格として採用され、「ISO/IEC1779：2000情報技術－情報セキュリティ管理実施基準」（以下、「ISO17799」という。）となった。（情報セキュリティマネジメントシステム（ＩＳＭＳ）の国際動向と取組みの実際 JIPDEC2002.9、URL http://www.isms.jipdec.or.jp/intre）

この「ISO17799」は「情報」に着目し、コンピュータ機器やネットワークを用いるいわゆる情報システムと、紙に記述された情報や言葉など、また当然情報システム上で取り扱われるデータとしての「情報」とを包含した広い範囲の情報セキュリティの管理基準であり、10の主な大項目と約130の中項目に区分けされた要求事項を定めている。

ＩＳＯではこの「ISO17799」を参考に、情報セキュリティを構築することを企業や自治体が自己責任で実施していくという位置づけとしている。一方、英国ではＩＳＯの採用にはいたらなかったが「BS7799」のパート２を用いて第三者認証制度を構築した。この第三者認証制度は品質管理「ISO9000」、環境マネジメント「ISO14000」でもおなじみであり、各企業や自治体がＩＳＯの要求事項に従った行動ができているかどうか、あらかじめ登録された第三者機関が審査認証する仕組みである。

## 2.3　世界のＩＳＭＳ制度の導入状況

いまやコンピュータウイルスやハッカーはインターネットを通じて世界中どこからでも襲ってくるものとなっており、自国だけ積極的に情報システムのセキュリティに取り組むだけでは限界がある。また自国の取り組みが遅れていると結果的に世界中に迷惑をかけることとなる。そのため情報セキュリティは環境問題などと同様に、世界中が足並みをそろえて取り組んでいく必要がある。

2002年３月時点で「ISO17799」をもとに自国の規格化を修了し、また「BS7799」に基づいた認証制度を取り入れている国は、イギリスをはじめオランダ、オーストラリア、ニュージーランド、ブラジル、チェコ、フィンランド、アイスランド、アイルランド、スウェーデン、ノルウェーである。

一方、まだ「ISO17799」を基に自国の規格化を実施していない先進国にはアメリカ、カナダ、ドイツなどがある。

このうち、ドイツはシステム監査を法制化するなど情報セキュリティには先進的な国であり、「BS7799」の認証制度も2000年12月に一部で自発的に実施されているが、ドイツでは古くから「ＩＴベースライン・プロテクション・マニュアル」が制定されており、このマニュアルが「ISO17799」を包含しているという立場を取っている。

一方、アメリカ、カナダは「ISO17799」は技術的に改善すべき点がかなりある、として自国規格化を実施していない。これは両国とも情報セキュリティの先進国という自負があるためと考えられる。カナダでは大蔵省（ＰＣＯ）のサイトでセキュリティポリシーなどを公開しており、実際に各組織が情報セキュリティの構築に取り組む際には参考となる。またアメリカでは標準技術局（ＮＩＳＴ）が組織的情報セキュリティマネジメントに有益な文書を無料で公開し（例；

SP-800-12 Computer Security Handbook, SP 800-26 Security Self-Assessment Guide For Information Technology System)、情報セキュリティの向上の支援を行っている。また、国際的にビジネスを展開している企業では、自社内に標準を作る必要性から「ISO17799」および認証基準である「BS7799」パート２を導入するところが出てきている。

## 2.4 日本の動向

日本では「ISO17799」が制定されるとそれに伴う国内規格である「JIS X 5080:2000 情報セキュリティ管理基準」（以下、「JIS X 5080」という。）を制定した。一方、以前より経済産業省（旧：通商産業省）の「情報処理サービス産業情報システム安全対策実施事業所認定制度」（以下、「安対事業者認定制度」という。）があり、一定の基準を満たした事業所を認証する制度を持っていた。このため「JIS X 5080」制定を機会に日本独自の認定制度を廃止し、国際基準に則った認証制度である情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度への移行を実施することとした。これが日本のＩＳＭＳ制度である。ＩＳＭＳ適合性評価制度は「BS7799 パート２」と考え方や主旨は同じであるが、「BS7799」の認証制度そのものではない。

2001 年４月から主に情報処理サービス産業情報システム安全対策実施事業所認定事業所からの移行を中心にＩＳＭＳ認証制度のパイロット事業を開始し、2002 年４月から本格的運用を開始した。2003 年３月３日現在、ＩＳＭＳ認証を取得した事業所は 91 にのぼっている。

（ＩＳＭＳ適合性評価制度のホームページ http://www.isms.jipdec.or.jp）

## 2.5 情報セキュリティ対応策の主眼の変化

経済産業省が実施していた安対事業所認定制度の安全対策基準は情報システムの主流が高価な大型コンピュータであり、堅牢な情報システムセンタの中に格納して地震、火災、空調機などのユーティリティの故障停止、コンピュータ自体の故障などから情報システムを保護することを主目的としており、どちらかというと物理的な対応策が中心となっていた。

一方、最近はシステムの小型化、またサーバ機を中心としたサーバクライアントシステムに移行し、一般の事務室の中に各種情報システム機器が存在するよう環境が変化する中で、情報セキュリティもホストコンピュータおよびシステムオペレータを中心とした限られた要員に限定されたものから、一般の従業員すべてを対象とするものへと大きく変化している。

そのため、「ISO17799」では主要な 10 項目として、次の要求事項を挙げている。

①情報セキュリティポリシー
②情報セキュリティ組織
③情報資産の分類管理
④人的セキュリティ
⑤物理的環境的セキュリティ
⑥通信および運用管理
⑦アクセス制御
⑧システム開発メンテナンス

⑨事業継続管理

⑩準拠

またＪＩＰＤＥＣが行った「情報セキュリティに関する調査」では、その中で重要視されるものが経営者が関与して作成する「情報セキュリティポリシー」や情報セキュリティの推進のための「情報セキュリティ組織」、従業員の教育や事故対応などを定めた「人的セキュリティ」など、人間を中心としたものとなっている。一方、「物理的環境的セキュリティ」は７番目とあまり重要視されておらず、時代環境の変化に伴い、対応の優先度も実際に変化してきている。

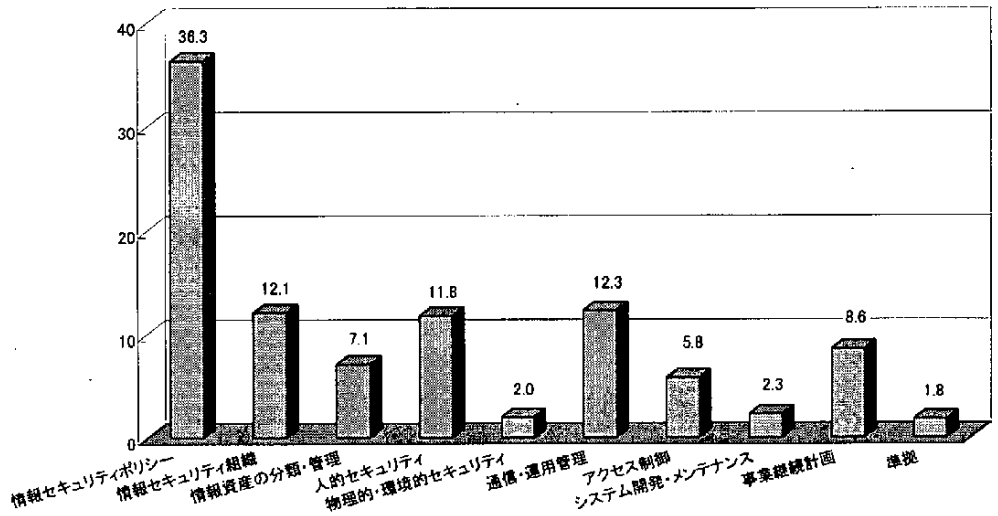


図２－１．ISMSの要素で一番重要視する要求事項

出典:「わが国における情報セキュリティの実態－「情報セキュリティに関する調査」集計結果(JIPDEC、2002.3)

## 2.6　ＩＳＭＳのカバーする範囲

現在情報セキュリティといえば「ISO17799」を真っ先に掲げるほど一般的になってきているが、リスクマネジメント全体からいうと、「ISO17799」が運用を中心とした一部分のみをカバーしていることは認識しておかなければならない。情報システムはそのライフサイクルを考えると情報システムを構築するにあたり、企画、開発、運用、破棄となるが、このうちＩＳＭＳ制度は「情報」に着目し、またその構築された情報システムの運用に着目した仕組みである。したがって 2002 年２月や４月に発生した銀行の合併などに伴う、システムの大きな統合事業に伴う事故は企画、開発などの観点が強い分野で起こったものであり、必ずしもこのＩＳＭＳ制度の導入だけではカバーできないものであることに留意する必要がある。

そのためＪＲＭＳでは企画、開発などに存在するリスクについてもその対象とし、情報システムに関するリスクのすべてをできるだけ網羅することを目指した。

ところで、セキュリティ管理対策の国際規格はこの他に大きなもので二つある。一つは 1999 年に制定された「ISO15408（IT Security Evaluation Criteria；JIS X 5070)」（以下、「ISO15408」という。）である。これは Common Criteria と呼ばれており、情報処理製品やシステムの信頼性を認証する制度である。

もう一つは「ISOTR13335 (Guideline for the Management of IT Security) (TRは技術情報テクニカルレポートの意味で、正式な規格ではなく参考情報扱い)」で、セキュリティポリシーの作成や、情報処理システムの運用に係わる人や情報処理機器の管理に関するものである。この「ISOTR13335」のリスク分析のアプローチは汎用性が高く、ＩＳＭＳ制度の中で情報資産を評価分類するときの脆弱性分析などに用いられることが多い。(注;よくＩＳＭＳの認証の際に情報資産の分類にあたり「ISO13335」でなければならないと勘違いする人が多いが、「ISO17799」ではそもそもリスク分析の手法そのものを定めておらず、そのため「ISO13335」以外の手法を用いてもよい。したがって、ＪＲＭＳを分析手法の一つとして用いることも推奨され、さらに合理的な手法であれば、自社で開発した手法を用いてもまったく問題ないのである。)

## 2.7 情報セキュリティ監査制度の発足

2003年3月現在、日本ではＩＳＭＳ制度に加えてさらに情報セキュリティを発展させるための取り組みが強化されることとなり、2003年4月から情報セキュリティ監査制度が新たに立ち上げられようとしている。この情報セキュリティ監査制度の発足につき、経済産業省情報セキュリティ監査研究会報告書中間報告（2003年1月29日）ではその背景を次のように述べている。

①情報システムの浸透度

まず情報システムの浸透度合いについては、中央省庁や自治体における業務や行政のサービスのコンピュータ化およびそれらに関連する情報の電子化が急ピッチで進められている。2002年8月には住民基本台帳ネットワークが稼働を開始し、さらに2003年度からは電子政府・自治体システムの本格的な稼働の開始が予定されていることを詠っており、政府や自治体という公共機関で大幅に情報システムへの依存度が向上したことが第一の理由である。次に企業間および企業と消費者の間の電子商取引の活用、高速なインターネットアクセス回線の普及に伴い、個人も含めたインターネットの利用の急激な増加がある。

②セキュリティ事故の深刻さ

一方、これらの情報技術や情報システム利用環境の急激な発展とは裏腹に、セキュリティ対策の不備に伴うさまざまな問題の発生が社会的に深刻な影響を与えるまでになっている。情報システムへの不正侵入、個人情報や機密情報の漏洩、情報システムに保存されている情報の破壊、ホームページ改ざん、システムダウンなどの情報セキュリティ事故により、国家、企業の経済的な損害のみならず、人権の侵害、企業活動の停止という社会的影響は無視できない。

③情報セキュリティ制度の整備

これらの環境変化を受け、情報セキュリティに関する制度整備は進んできている。「ISO15408」、ＩＳＭＳなどの認証制度、暗号技術評価、インシデント情報の共有化（JIPDEC、IPA）などがある。

④情報セキュリティ監査の立ち遅れ

これらの環境整備の中で、自らが独立した第三者の専門家から情報セキュリティの有効性の評価を受ける「情報セキュリティ監査」の分野が大きく立ち遅れていることが判明した。

情報セキュリティ監査はコーポレートガバナンスの関連でもあるリスクマネジメント体制の有効性、内部統制の有効性を確保するためにも不可欠なマネジメントプロセスの構成要素である。

以上のような認識から経済産業省は 2003 年4月から情報セキュリティ監査制度を開始する方

針を決定した。
(http://www.meti.go.jp/policy/netsecurity/index.html)

## 2.8 情報セキュリティ監査の特徴

この情報セキュリティ監査は新たに独自のものを設けるのではなく、ＩＳＭＳ制度の下支えをする制度と位置づけられている。まずＩＳＭＳも情報セキュリティ監査制度も準拠する基準は「JIS X 5080」であり、まったく同じものである。

それではなぜ新たに情報セキュリティ監査を考える必要性が生じたかをみると、一番大きい理由は、多種多様な組織の多種多様なニーズに応えることが挙げられる。中央省庁や都道府県、市町村など電子自治体および住民基本台帳の運営の主体もその人員規模、情報システムの対応、拠出可能な予算の規模などまったくさまざまである。また企業も含めて考えれば、監査を受けることの重要性が高まるにつれ、情報セキュリティ対策の不備の指摘を求めるものや、商取引の相手先からの情報セキュリティの有効性の保証を求めるものなど、そのニーズが多様化してきている。これらのニーズに柔軟に対応できるようにし、継続的に監査を導入する環境を整備するために、ＩＳＭＳ制度とは別に情報セキュリティ監査制度を開始することとしている。

いわば、ＩＳＭＳ制度と情報セキュリティ監査とは役割分担を演じることとなる。具体的にいえば情報セキュリティ監査はＩＳＭＳと同じ「JIS X 5080」を用い、その一部分のみ、また他の基準も利用しながら保証または助言を行っていくという幅広いニーズに応えることを目的としている。

情報セキュリティ監査制度の発足にあたって、一番想定しうる利用の効果は、「情報セキュリティ監査基準」の一部の、たとえば「アクセス基準」の技術的な部分にのみ重点的な監査を行うことなど、企業や自治体の現状を踏まえた身の丈にあった監査の受診が可能となることである。またＩＳＭＳの準拠性監査を実施し、一定のレベルに達したと判断した時点でＩＳＭＳを取得する、といったレベルアップを目指す監査の受診も可能である。

## 2.9 情報セキュリティ監査の留意点

電子自治体および住民基本台帳などの公的業務への情報セキュリティの第三者評価を実施するというニーズに対し、この情報セキュリティ監査はまず適応することが求められる。一方、監査を受ける主体としてもどこの部分の監査を受け、結果どのようであったかについては公的機関であれば情報公開をすることが当然ながら求められる。情報セキュリティの対策強化に本格的に取り組んでまだ日が浅いところであり、ＩＳＭＳの取得には時間がかかるところであっても、この情報セキュリティ監査により、たとえばウイルス対策は十分である、あるいはアクセス制御のペネトレーションテストだけは修了している、といった部分をどの水準で実施できているかといった情報を公開することは、多くの市民に安心感を与える。欲をいえば求められる標準点を早く達成してほしいというところであるが、まずはリスク分析の実施により弱点を知っておくことがリスクマネジメントの基本的行動として必要であり、継続的改善というマネジメントシステムの思想に則り、その後向上させていくことでよいと考える。なお、情報開示にあたっては、具体的な

内容そのものの公開（たとえばセキュリティホールの内容など）は新たな悪意の攻撃の的となるため不要であるが、概要は公開する必要があると考える。

なお、「2.6　ＩＳＭＳのカバーする範囲」でも述べているが、ＩＳＭＳおよび情報セキュリティ監査はあくまで運用を中心とした部分で適用されるものであるため、情報システムの企画、開発といった分野は対象外となる。そのため、従来からあるシステム監査がすべて情報セキュリティ監査にとって変わるものではないことに留意する必要がある。監査についていえば、今後は1985 年に制定されたシステム監査基準と情報セキュリティ監査基準との整合性を図る必要性があり、今後検討が開始される予定である。

また、企画、開発といった分野についての監査あるいは管理基準としては、ＩＴガバナンス、ＣＯＢＩＴ、プロジェクトマネジメントなどの各種手法を用いることが望ましい。

なお、運用面を中心とした監査であっても監査を受ける側の要請があれば他の基準に準拠して実施することにはなんら問題はない。

参考になる基準としては「システム監査基準;1985 年１月」、「情報システム安全対策基準;1995 年８月」「コンピュータウイルス対策基準；1995 年７月」、「コンピュータ不正アクセス対策基準；1996 年８月」（以上経済産業省）、「情報通信ネットワーク安全・信頼性基準；1987 年」（総務省）、「情報システム安全対策指針；1997 年」（警察庁）などがある。また金融関係では（財）金融情報システムセンター（ＦＩＳＣ）が「金融機関等コンピュータシステムの安全対策基準」を発行している。

なお、今後国としては電子政府に関連するシステムとして、庁内ネットワークシステムをモデルに「電子政府情報セキュリティ管理基準モデル（庁内ネットワークシステム）」を策定していくこととしている。なお、電子政府に関連するシステムとしては、この他に公開サーバネットワークシステム、認証局システム、インターネット以外の外部接続システムなどがある。

## 2.10　今後の情報セキュリティの必要性

2003 年１月 25 日には韓国をはじめ多くの国でＳＱＬサーバのセキュリティホールを狙ったウイルスが多発し、インターネットの利用が事実上困難になる事件が発生した。（「1.3」参照）

また、個人がインターネット環境に常時接続しているところをサイバーテロリストに狙われてなりすまされ、一時はアメリカ当局から当該個人が犯人扱いされるという事件も発生している。従来の企業や自治体の情報システムは企業の中の閉じた系であり、そのセキュリティも限られた範囲を想定すればよかった。いまや企業や自治体の中心となる情報システムは外部との接続を前提とした基盤の上に構築されており、いやがおうにも他組織、個人との接続があり、開かれた系である。開かれた系ではどこか弱い一か所から全体に弱点が伝播するため、今後は自らも一定のレベルに情報セキュリティを保つことと同様に、接続している他者にも同様のレベルを求めていくことが必要になる。情報技術の発展は今後も続くであろうし、またウイルスやハッカーあるいはコンピュータを悪用した犯罪などの人為的な悪意もまた増大することが予想される。そのため被害者にならないことに加え、加害者にもならないために、組織はこれまで以上に情報セキュリティに留意することが必要になる。

# 3．ＪＲＭＳの実証実験結果

## 3.1　モデル企業のケース

2002年３月に「JIPDECリスクマネジメントシステム（ＪＲＭＳ）のあり方に関する研究（ＪＲＡM2002)」を発表したが、このＪＲＭＳを現実の経営の場に適用した場合の有効性を確認する必要性を検証することが重要な課題であった。そこで、ＪＲＭＳの実践的な意味（有効性・使いやすさ等）を探り、効果的な手法にするための改善の余地を見出す目的で、モデル企業の協力を得てこの点の解明を試みる必要性がリスク対策検討委員会(以下、「委員会」という。)において確認され、2002年６月にモデル企業の募集を行うことになった。

委員会の目的に協力してもらうとしてもＪＲＭＳの質問項目数に問題があった。ちなみに総質問項目数（発表時）は1,018であり、情報システム部門（以下、「ＩＳ部門」という。）対象の質問項目はユーザ部門に関する１問を除く99.9%の1,017問、経営者層も318問となっていた。経営者層として300を超える質問に回答する意味があるのか、現実的に可能なのかどうかについて委員会において疑問が提示され、検討の結果、質問項目数の減少ならびに表現の見直しを含めた作業を行い、経営者層の場合、質問項目数は50問に落ち着いた。

さらに、委員会としては、モデル企業の協力を得るにあたり経営者層、ＩＳ部門、ユーザ部門それぞれの回答担当者が投入するマンアワーの負担の大きさをも考慮する必要があった。モデル企業の公募において､幸いにもＡ社の協力を得ることができた。(契約関係からモデル企業名は伏せさせていただく。)

ＪＲＭＳの実証実験のため、Ａ社の担当者３名に６月に行われた委員会に参加していただき、実証実験の趣旨ならびにＪＲＭＳ質問票の内容ならびに回答の仕方、レーダーチャートの描き方等について解説をした。その上で委員会に提出していただくアウトプット（回答の方式）についての協議を行った。

その際、経営者層、ＩＳ部門、ユーザ部門別にＪＲＭＳの質問票に回答を記入し、それをグラフ化するまでの一連のプロセスを説明した。１つのディレクトリの下に４種類のファイルを用意した。すなわち、経営者層の回答用、ＩＳ部門の回答用、ユーザ部門の回答用、それにグラフ作成用のファイルである。

回答用のファイルは個別質問のシートと集計用の「集計シート」から構成されている。個別質問のシートへの回答結果は自動的に計算されて集計シートに入ると共に、各回答ファイルの集計シートから自動リンクでグラフ作成用ファイルの集計シートに入ることになっている。さらに､グラフ作成用のファイルの各シートでグラフが描けることになる。いわば､各回答ファイルに回答を記入すれば、一応、グラフが自動的に作成できるようにしておいた。

Ａ社からは８月中旬に回答をいただいた。その結果、グラフ作成まで一連の作業が展開されており、並々ならぬ協力をいただいた。ただ、委員会において用意した自動化のプログラムが回答者数の変更等に十分対応していなかったことなどが確認され、プログラム改善のための貴重な情報となった。その後の委員会において回答結果に対する委員相互による意見交換を行い、10月下旬に委員会としての総合的な回答である「モデル企業回答結果についての評価」（報告書）を作成し、報告会を行うことにした。

### 3.2　A社の回答者から提示された見解とそれへの対応

報告会当日は、A社側から経営者層を代表した役員１名、ＩＳ担当部長職１名、リスク対応部局から２名の計４名が出席された。まず、委員会側が上記報告書を基に分析結果の報告を行った。その後、A社側よりＪＲＭＳの質問項目・回答の仕方・委員報告に対する率直な感想を頂戴した。

A社役員からは、「回答の仕方に関し、会社ではそれぞれの部署に責任・権限が分かれており、質問項目によっては『わかりません』、『知りません』、『関係ない』といった選択肢がないのはどうか」という課題の提起が行われた。たしかにこの点については、評価基準の選択肢が用意されていないため、そうした場合すべてが＜Ｎｏ＞となってしまい、他の質問への回答に影響が出てくることになる。そのほか、質問によって回答が＜Ｙｅｓ／Ｎｏ＞の場合に自動的に＜Ｙｅｓ＞は３、＜Ｎｏ＞は０となる項目と、０～３で評価する項目とを組み合わせてレーダーチャートで示すのが妥当かどうかも疑問視された。この点は評価基準の明確さに関わることになる。それゆえ、委員会での今後の検討課題の一つとなった。

さらに、「会社としての経営に関わるレベルとＩＳ部門・ユーザ部門の運営に関わるレベルと２つに質問を分けるべきである」という指摘を頂戴した。この点は、見直し作業で検討することになり、対応することとなった。

ところで、ＩＳ部門の感想・意見としてＩＳ担当部長よりいくつかの指摘がなされた。その一つに次のような見解があった。すなわち、総じて回答担当者にとり「リスクマネジメントの現状を悪く評価し、危機感を煽る」のではないかといった指摘である。経営ならびに管理に関する質問に対しては、担当する部署以外の者には「判断が難しいため、評価することに意味があるのか」といった指摘もあった。特に、情報関係の質問については、「それ以外の部署の者に回答を求めても適切な回答がかえってくるとは限らない。回答者を選別するのも困難であり、事務局で経歴や経営と情報についてある程度の考えを持っている者を選別したが、回答者の経歴や担当内容が結果に如実に表れ、シビアに考えるか、楽観的に考えるかによっても回答結果にバラツキが生じる。」評価基準との関係から回答するにあたり「回答しているうちに自虐的になる」といった感想も寄せられた。こうした側面については、評価基準の明確化が不可欠となる。

なお、質問項目について、ＩＳ担当部長から、「質問項目には膨大な情報が入っており、ブロックごとに具体的な評価を行わないと、よいデータにならない」という貴重な意見が提示された。回答に際して、リスク対応に関して悲観的・楽観的な側面が生じやすいことがあったが、「できているのではないか」といった判断なり期待度によって個人差が生じることがある、という指摘もあった。この点は、質問項目によっては、経営者とＩＳ部門、ＩＳ部門とユーザ部門等で回答に違いが出ていることが回答結果から確認できた。

この他、数々の疑問・意見が寄せられたが、委員会としては、基本的に質問項目に回答することによりそれぞれの部署の担当者ならびに関係者に業務に関わるリスクに対して共通認識を有してもらうことができ、また適切・迅速な対応が可能になることの重要性を指摘した。

一般に、企業では人事異動が定期的に実施されており、「人が代わった時には引継ぎを行うにしても、前任者と同様に業務内容を遂行できるかどうか」という側面があることから、リスク対応のための文書化・明文化・マニュアル化が必要であることに言及した。（この点に関しては、日本の企業では、マニュアルの作成には熱心であるが、一旦できあがると本棚に置かれ、関係者だけ

がその存在を知っており、人が代わると、やがてマニュアル自体の存在も忘れ去られるといった事態も見られた残念なケースもある、といった情報交換も行われた。）

### 3.3　A社のＪＲＭＳに対する評価

委員会として考えなければならなかったことは、ＪＲＭＳがリスクマネジメントの視点から手法として有効かどうか（仮説）であった。その検証のために実証実験を行ったわけである。「モデル企業回答結果についての評価」（報告書）の質疑応答において、今回の実証実験に関し辛口ながら積極的かつ肯定的な評価が寄せられた。すなわち、リスクチェックのためのこれだけの仕組みはなかなかなく、ここまでできあがっているのだから有効利用すべきである。また、ＪＲＭＳを資格認定とセットにし、評価制度にもっていくことも一案である、とされた。

また、ＩＳ担当部長からは、「ＪＲＭＳの質問項目を勉強し、社内での活動に活用させてもらい、回答者のバラツキの原因が何によっていたかが理解できた。今後の社内における改善計画にとり役立った」という意見を頂戴した。

### 3.4　委員会としての対応と総括

委員会としては、今回の実証実験の回答結果を踏まえ、現実の経営では、回答結果に基づくレーダーチャートだけから組織としての対応の傾向を読み取ることができないことに留意した。特記すべき事項は以下のとおりである

①経営者層・ＩＳ部門・ユーザ部門ではそれぞれ回答項目数が異なるため、レーダーチャートの評価結果には、若干の誤差があること

②回答者の役職上の責任範囲が異なることから、質問項目の受け止め方に差異が生じうること

③質問項目の理解の仕方（正確か否か、厳しく捉えるか否か）・回答者の判断（的確か否か、組織としての判断か・個人的な印象か）により、回答にバラツキが生じうること

④同じ質問であっても回答者間での認識ギャップがあること

⑤バラツキや認識ギャップの存在を踏まえ、それぞれの部門において意見交換を行い、実態についての情報を共有し共通認識を有すること

⑥情報を共有したうえで、再度回答を持ち寄り、レーダーチャートを描き、リスク対応の実態についての傾向を組織として捉え、リスクマネジメントに資すること

総括としてみると、今回のＡ社の協力により、委員会としてＪＲＭＳの有効性について仮説検証ができ、しかも一定の評価を得ることができた。

しかしながら、ＪＲＭＳの質問項目の妥当性・プログラムの使いやすさ・回答に対する評価基準等について改善すべき課題を把握することができ、方向性が見えた有意義な実験であったといえる。

リスク対策検討委員会としてＡ社のご協力に深く感謝の意を表します。

# 4．ＪＲＭＳ2003の構成

## 4.1　ＪＲＭＳ2003の構成

ＪＲＭＳの目的は、組織全体のリスク対応の実態（現状）を認識し、情報システムに関わるリスクマネジメントのあるべき姿とのギャップを質問項目への回答結果を通して確認し、組織として効果的なリスクマネジメント体制の構築に資することにある。

情報システムに関わるリスク対応に関しては、これまで関係諸機関において種々のガイドラインなり基準等が提示されている。ＪＲＭＳは、「JIS Q 2001：2001　リスクマネジメントシステム構築のための指針」（以下、「JIS Q 2001」という。）をベースにおきながら、ＪＲＡＭの方法論に基づき、情報システムにおけるリスクを対象に展開してきた。

ところでＩＳＭＳ適合性評価制度が情報処理サービス業においてかなりの認知度を有している（74.4％：『わが国における情報セキュリティの実態「情報セキュリティに関する調査」集計結果』日本情報処理開発協会、P.87）。このＩＳＭＳとＪＲＭＳの関連性についてはすでに「２．情報セキュリティに関する最近の動向」において論述されているように、ＩＳＭＳは情報システムを利用する組織が示されている要求事項に適った行動ができているか、ＩＳＭＳ認証基準に則っているか否かを問うもので、当該基準を満たしていれば認証が与えられる。認証規格に対してセンシティブなわが国の組織では、認証が与えられれば、それで情報セキュリティは万全であるかのような印象が持たれやすい。

しかし、それぞれの認証取得企業における実態はどうなのか。たとえば、ＨＡＣＣＰの認証を得ていた雪印乳業のケースを想起するのがよい。認証を得ていることがすべての要求事項を実際に満たしていることと同じであるのかどうか。こうした側面は、情報セキュリティの場合も同様である。

現代社会において、組織としてリスク対応の実態を検証することは不可欠である。ＩＳＭＳとギャップ分析に視点を置いたＪＲＭＳとは目的が異なっている。さらに重要なのは、ＩＳＭＳがカバーしている情報リスクの領域が何であるのかの明確な理解である。この点は、前述の「2.6　ＩＳＭＳのカバーする範囲」を熟慮するとともに「4. 4　ＪＲＭＳとＩＳＭＳの相違点」を参照されたい。

さて、ＪＲＭＳに関する今年度の委員会での検討事項の特徴は、実証実験において指摘された点を踏まえ、組織の全般的なリスク対応と情報システムへの対応策に関する側面の二つから構成し直した点にある。第一は、経営に関わるリスクマネジメントシステムの部分である。経営全般に関する部分では情報システム部門の責任者を加えながら回答を行うが、回答の集計担当部署としてリスクマネジメント（ＲＭ）部門を当てる形に修正した。したがって、経営者層（ＣＥＯ、ＣＯＯ、ＣＦＯ等）、リスクマネジメント担当役員（たとえばＣＲＯ）、情報システム担当役員（ＣＩＯ）、ユーザ部門の役員が組織のリスクマネジメント全般についての実態を把握するため、チェックを行うことになる。

第二は、経営全般に対する実態を踏まえながら、情報システム担当部門が情報リスク対応を行う点である。現代の組織は相互依存関係が情報システムを通してこれまで以上に密となっており、一つの部署の問題（制約条件）が経営そのものに及ぶようになっている。このような現在の経営

環境下において、情報システムリスクマネジメント責任者がユーザ部門との接点のもとでリスクに対応することが非常に重要となってきている。

一般的に、経営者層は経営全般のリスクを把握する責務があり、リスクマネジメント部門（担当責任者）は経営に関わるリスクの分析・対応に対して責務があるとされている。しかし、情報システムに関わるリスクがすべてに作用する現在の環境下において、情報システム担当部門が情報システムだけのリスクに目を配るだけでは十分とはいえない。むしろ経営全般に関わるリスクについても理解し、リスクマネジメント部門との協同においてリスク対応を計ることが必須といえるのである。

リスクマネジメントの実践には関係者の共通認識が不可欠であり、とりわけ経営者層のコミットメントが重要である。ＪＲＭＳの質問項目では、経営者層が回答する（関与する）ことによりリスク対応に関するコミットメントを得ることになっている。これにより情報システムに関わるリスクマネジメントの有効性が確保できるものと思われる。

以下は、これまでの環境変化を考慮に入れながら、ＪＲＭＳの見直し作業によりまとめ上げた成果である。

### 4.1.1　2001 年度報告書からの主な修正項目

2001 年度の研究成果として、「ＪＩＰＤＥＣリスクマネジメントシステム（ＪＲＭＳ）のあり方に関する研究（ＪＲＡＭ2002)」をまとめ発表した（2002 年３月)。

しかし、情報システムを利用する組織の活発な活動は情報システムに対する依存度をますます高め、経営環境における情報システムの変化を著しくさせている原因の一つとなっている。

このような経営環境と情報システムの変化に伴い、情報システムに係わるリスクは組織全体に大きな影響を与えるだけでなく、大きな社会問題に発展する要因となる可能性が強くなっているのが現状である。

そのため、情報システムに係わる個々のリスクを個々の問題として捉えるだけではすまされなくなっており、個々のリスクが組織全体に与える影響を常に考慮することが、リスク対応上必要不可欠となっている。

たとえば、大手都市銀行のシステム障害の問題、個人情報の数々の漏洩問題、そしてさまざまなウイルス、不正アクセスの問題などが顕著なケースとして身近に発生している。

このような環境の変化を踏まえて、2001 年度報告書の内容の見直しを行い、修正を加えた。

2001 年度報告書を見直した結果の主な修正項目は以下のとおりである。

①質問項目構成の改善
②監査項目の独立
③ＪＲＭＳのリスク分析、リスク対策の独立
④リスク対策における実施基準の重視

### 4.1.2　主な修正点の概要

2001 年度報告書を見直し検討した結果の、項目ごとの主な修正点の概要は以下のとおりである。

表４－１．2001年度／2002年度　質問項目の大項目と全質問数　比較表

| 2001年度 | |
|---|---|
| Ⅰ | 経営とリスクの関係 |
| Ⅰ-1 | 経営環境とリスクマネジメント |
| Ⅱ | ＪＲＭＳにおけるリスクマネジメント計画 |
| Ⅱ-1 | ＪＲＭＳの計画 |
| Ⅱ-2 | ＪＲＭＳの実行組織 |
| Ⅱ-3 | ＪＲＭＳの維持 |
| | |
| Ⅲ | ＪＲＭＳのリスク分析 |
| Ⅲ-1 | ＪＲＭＳのリスク分析 |
| Ⅲ-2 | 情報セキュリティポリシーのリスク分析 |
| Ⅲ-3 | 情報システムのリスク分析 |
| | （1）情報システムのリスク分析 |
| | （2）情報システム総合企画 |
| | （3）システム開発 |
| | （4）システム運用 |
| | （5）不正アクセス・コンピュータウイルス関連 |
| | （6）災害 |
| | （7）障害 |
| | （8）アウトソーシング |
| Ⅳ | ＪＲＭＳにおけるリスク対策 |
| Ⅳ-1 | リスク対策における情報セキュリティ |
| Ⅳ-2 | 情報システムのリスク対策 |
| | （1）情報システム総合企画 |
| | （2）システム開発 |
| | （3）システム運用 |
| | |
| Ⅳ-3 | 不正アクセス |
| Ⅳ-4 | コンピュータウイルス関連 |
| | （1）コンピュータ犯罪 |
| | （2）コンピュータウイルス |
| | （3）Ｅ－Ｃｏｍｍｅｒｃｅ |
| | （4）電子メール |
| Ⅳ-5 | 災害対策 |
| Ⅳ-6 | 障害対策 |
| Ⅳ-7 | アウトソーシング関連リスク対策 |
| Ⅳ-8 | その他関連項目 |
| Ⅳ-9 | バックアップ |
| Ⅳ-10 | 緊急時対策 |
| Ⅳ-11 | リスクファイナンス　（廃止） |
| 全質問数合計 | １，０１８ |

| 2002年度 | |
|---|---|
| Ⅰ | 経営とリスクの関係 |
| Ⅰ-1 | 経営環境とリスクマネジメント |
| Ⅱ | ＪＲＭＳにおけるリスクマネジメント計画 |
| Ⅱ-1 | ＪＲＭＳの計画 |
| Ⅱ-2 | ＪＲＭＳの実行組織 |
| Ⅱ-3 | ＪＲＭＳの維持 |
| Ⅱ-4 | ＪＲＭＳのリスク分析 |
| Ⅱ-5 | ＪＲＭＳのリスク対策 |
| Ⅲ | 情報システムのリスク分析 |
| Ⅲ-1 | 情報セキュリティポリシーのリスク分析 |
| Ⅲ-2 | 情報システムのリスク分析 |
| | （1）情報システムのリスク分析 |
| | （2）システム開発 |
| | （3）システム運用 |
| | （4）アウトソーシング |
| Ⅲ-3 | 情報システムの個別リスク分析 |
| | （1）不正アクセス・コンピュータウイルス関連 |
| | （2）災害 |
| | （3）障害 |
| | |
| Ⅳ | 情報システムにおけるリスク対策 |
| Ⅳ-1 | リスク対策における情報セキュリティ |
| Ⅳ-2 | 情報システムのリスク対策 |
| | （1）情報システム総合企画 |
| | （2）システム開発 |
| | （3）システム運用 |
| | （4）アウトソーシング |
| | （5）システム監査　（新） |
| Ⅳ-3 | 不正アクセス・コンピュータウイルス関連 |
| | （1）コンピュータ犯罪 |
| | （2）不正アクセス |
| | （3）コンピュータウイルス |
| | （4）Ｅ－Ｃｏｍｍｅｒｃｅ |
| | （5）電子メール |
| Ⅳ-4 | 災害対策 |
| Ⅳ-5 | 障害対策 |
| | |
| Ⅳ-6 | その他関連項目 |
| Ⅳ-7 | バックアップ |
| Ⅳ-8 | 緊急時対策 |
| | |
| 全質問数合計 | １，００４ |

1．質問項目構成の主な改善の概要

2001 年度、2002 年度の質問項目の大項目と全質問数を表４－１に示したが、主な改善の概要は次のとおりである。

（1）質問項目構成の改善

質問項目の構成を次のように整理し、全社的組織関連と情報システム関連とを分割した。

表４－２．ＪＲＭＳ質問構成

| | |
|---|---|
| Ⅰ | 経営とリスクの関係 |
| Ⅱ | ＪＲＭＳにおけるリスクマネジメント計画 |
| Ⅲ | 情報システムのリスク分析 |
| Ⅳ | 情報システムにおけるリスク対策 |

「Ⅰ」・「Ⅱ」は全社的組織関連、「Ⅲ」・「Ⅳ」は情報システム関連とした。

2001 年度は全社的組織関連と、情報システム関連が明確に分割されていなかった。

情報システムのリスクマネジメントを考える場合、情報システムのリスクが組織全体に与える影響を把握することがリスク対策を検討する上で重要であり、単に情報システムのリスクのみではなく、組織全体のリスクを捉えることが必須であることを考慮した。

（2）ＪＲＭＳの実行組織とリスクマネジメント体制の例

質問項目「Ⅱ－２．ＪＲＭＳの実行組織」に示された実行組織は、表４－３のように整理することができる。

表４－３．ＪＲＭＳの実行組織

| 組織名 | 実行担当 |
|---|---|
| 全社的リスクマネジメント組織 | リスクマネジメント担当役員<br>リスクマネジメント推進組織<br>リスクマネジメント担当者 |
| 情報システムリスクマネジメント組織 | 情報システムリスクマネジメント担当者<br>情報システムリスク管理者<br>情報システム運用管理責任者<br>情報セキュリティ対策推進組織<br>情報セキュリティ管理者 |
| ユーザ組織 | 適用業務別オーナ<br>ユーザ部門リスク担当責任者 |

さらに、これらの実行組織を踏まえたリスクマネジメント体制の一例を示すと、図４－１のようになる。

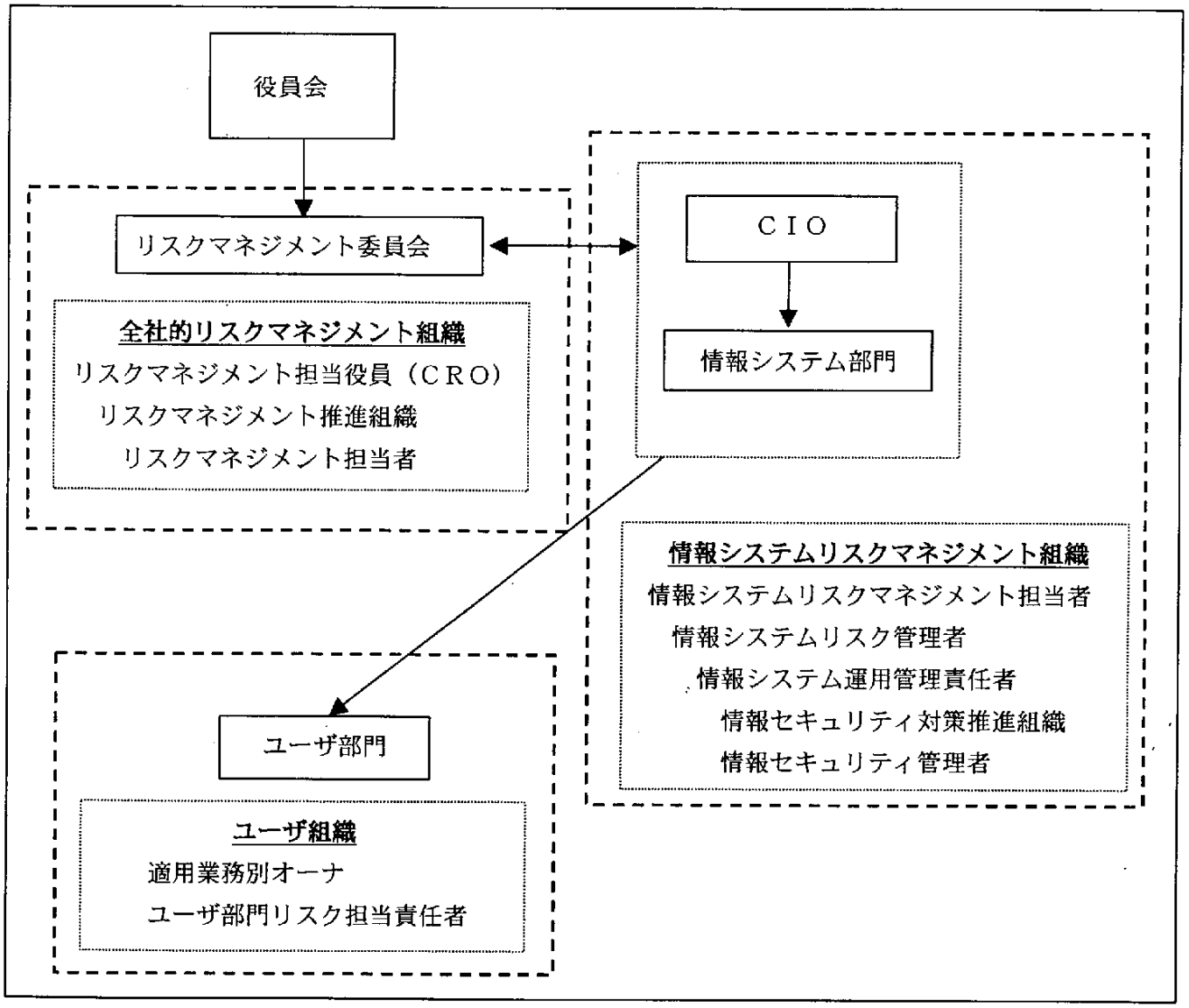


図４－１．リスクマネジメント体制例

（３）ＪＲＭＳの運用

リスクマネジメント体制の例に基づくＪＲＭＳの運用は、理想的には次のように行うことが望ましい。

・全社的リスクマネジメント組織

全社的リスクマネジメント組織（例：リスクマネジメント委員会）は役員会の意図を受け、リスクマネジメント担当役員（ＣＲＯ）が運営する。（ＣＲＯが不在の場合は、役員のうち適任者を役員会で任命する）。

・情報システムリスクマネジメント組織

情報システムリスクマネジメント組織は、情報システム担当役員（ＣＩＯ）または役員会で任命した適任者（以下、「ＣＩＯ等」という）の指示に従い、情報システムリスクマネジメント担当者が運営する。

ただし、ＣＩＯ等は情報システムリスクマネジメント担当者を兼務することができる。

・ユーザ組織

ユーザ組織はＣＩＯ等の指示に従い、業務別オーナが運営する。

・ＣＩＯ等の役割と責任

「Ⅰ」・「Ⅱ」はＣＲＯ、「Ⅲ」・「Ⅳ」はＣＩＯ等が質問項目全体を適切に運用する役割と責任を持つ。

このＪＲＭＳでは後述「4.3.3　ＪＲＭＳ推進の責任者」に指摘するように、実際の場における推進組織の責任はＣＩＯが負う。

（4）質問項目構成内容の修正

質問項目構成内容の修正点は次のとおりである。

・「Ⅱ－4．ＪＲＭＳのリスク分析」と「Ⅱ－5．ＪＲＭＳのリスク対策」をまとめて、「Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画」の下位構成とした。

・「Ⅲ」は「Ⅲ．情報システムのリスク分析」とし、「（2）情報システム総合企画」を削除した。

・「Ⅲ．情報システムのリスク分析」に「Ⅲ－3．情報システムの個別リスク分析」を追加し、「（1）不正アクセス・コンピュータウイルス関連」、「（2）災害」、「（3）障害」をその下位構成とした。

・「Ⅳ」は「Ⅳ．情報システムにおけるリスク対策」とし、「Ⅲ．情報システムのリスク分析」の関連を明確にした。

・「Ⅳ－2．情報システムのリスク対策」の下位構成に、「（4）アウトソーシング」、「（5）システム監査」を加えた。

・「Ⅳ－3．不正アクセス」と「Ⅳ－4．コンピュータウイルス関連」をまとめ、「不正アクセス」を下位構成とした。

・「Ⅳ－7．アウトソーシング関連リスク対策」は「Ⅳ－2．情報システムのリスク対策」の下位構成としたため、削除した。

・「Ⅳ－11．リスクファイナンス」は「Ⅱ－5．ＪＲＭＳのリスク対策」の中に含めて削除した。

2．監査項目の独立

リスクマネジメントの遂行上システム監査は重要な業務であることから、「Ⅳ－2．情報システムのリスク対策」の下位構成として、「（5）システム監査」を独立させた。

「Ⅳ－2－（5）システム監査」の質問項目大項目のキーワードと質問数は次のとおりである。

| | |
|---|---|
| 大項目のキーワード | 1．実施基準 |
| | 2．監査 |
| | 3．監査基準 |
| 質問数 | 11 |

3．ＪＲＭＳのリスク分析、リスク対策の独立

ＪＲＭＳのリスク分析とリスク対策を分離独立させ、関連を明確にした。主な理由は次のとおりである。

・組織全体としてどのようなリスクに取り囲まれているのかを明確にする（分析）。

・リスク対策を考える場合、個別のリスク対策としてそれぞれ異なる対策も必要であるが、組織全体として共通に実施する方が効果的である対策もあるため、これらをまとめた。

・従来はリスク対策のチェックリストに重点が置かれてきたが、組織や情報システムの多様性を踏まえ、対策の前にリスク分析の実施を重視した。

・網羅的な対策のチェックをやめ、リスクに対応した対策の選択が可能なようにした。したがって、リスク分析の結果、対応策の評点の重み（ウエイト）付けを変更可能とした。

それぞれの質問項目大項目のキーワードと質問数は次のとおりである。

（1）「Ⅱ－4．ＪＲＭＳのリスク分析」質問項目大項目のキーワードと質問数

| | |
|---|---|
| 大項目のキーワード | 1．リスク分析の仕組み |
| | 2．リスク分析の体制 |
| | 3．リスク分析の実施 |
| | 4．リスク分析（災害） |
| | 5．リスク分析（事故） |
| | 6．リスク分析（情報システム） |
| | 7．リスク分析（経営） |
| | 8．リスク分析（政治・経済・社会） |
| 質問数 | １２５ |

（2）「Ⅱ－5．ＪＲＭＳのリスク対策」質問項目大項目のキーワードと質問数

| | |
|---|---|
| 大項目のキーワード | 1．リスク対策の体制 |
| | 2．財務的対応 |
| | 3．リスク対応のための組み合わせ |
| | 4．テロ |
| | 5．人命損失 |
| 質問数 | ２６ |

4．リスク対策における実施基準の重視

実施基準を重視し、リスク対策はすべて実施基準に基づいて行うことを基本とし、その位置づけを明確にした。

（1）「Ⅳ－1．リスク対策における情報セキュリティ」への質問項目の追加

| |
|---|
| Q　実施基準に情報システム総合企画のリスク対策を定めていますか？ |
| Q　実施基準にシステム開発のリスク対策を定めていますか？ |
| Q　実施基準にシステム運用のリスク対策を定めていますか？ |
| Q　実施基準にアウトソーシング関連のリスク対策を定めていますか？ |
| Q　実施基準にシステム監査を定めていますか？ |
| Q　実施基準にコンピュータ犯罪対策を定めていますか？ |
| Q　実施基準に不正アクセス対策を定めていますか？ |
| Q　実施基準にコンピュータウイルス対策を定めていますか？ |
| Q　実施基準にＥ－Ｃｏｍｍｅｒｃｅ対策を定めていますか？ |
| Q　実施基準に電子メール利用対策を定めていますか？ |
| Q　実施基準に災害対策を定めていますか？ |
| Q　実施基準に障害対策を定めていますか？ |
| Q　実施基準にその他関連項目（経営リスク、政治、経済、社会リスク等）を定めていますか？ |
| Q　実施基準にバックアップ対策を定めていますか？ |
| Q　実施基準に緊急時対策を定めていますか？ |

（2）「Ⅳ－2」以降への関連項目の追加

上記「実施基準に…のリスク対策を定めていますか？」の質問項目を次の各大項目の最初にそれぞれ追加した。

「Ⅳ－2．情報システムのリスク対策」のうち、

「（1）情報システム総合企画」

「（2）システム開発」

「（3）システム運用」

「（4）アウトソーシング」

「（5）システム監査」

「Ⅳ－3．不正アクセス・コンピュータウイルス関連」のうち、

「（1）コンピュータ犯罪」

「（2）不正アクセス」

「（3）コンピュータウイルス」

「（4）Ｅ－Ｃｏｍｍｅｒｃｅ」

「（5）電子メール」

「Ⅳ－4．災害対策」

「Ⅳ－5．障害対策」

「Ⅳ－6．その他関連項目」

「Ⅳ－7．バックアップ」

「Ⅳ－8．緊急時対策」

（3）実施基準を重視した質問項目大項目のキーワードの例

「Ⅳ－2－（1）情報システム総合企画」大項目のキーワード

| | |
|---|---|
| 大項目のキーワード | 1．実施基準 |
| | 2．ＩＴ戦略 |
| | 3．ＩＴ計画 |
| | 4．組織体制・機能 |
| | 5．スタッフ |
| | 6．財務 |
| | 7．管理（文書化を含む） |
| | 8．モニタリング |

## 4.2 判定基準の見直し

4.2.1 ＪＲＭＳ質問項目の達成度判定の考え方

1．判定基準での修正点

2001年度に作成した質問票を使って実証実験を行ったが、2002年度の委員会活動として、この回答過程で得られた回答者からのコメントを反映し、ＪＲＭＳ質問項目の達成度判定の考え方の修正を行った。その主要なポイントは、次のとおりである。

1）＜D／K（知らない）＞の追加

企業規模が大きくなると、リスクマネジメントの機能がいろいろな組織に分散されており、回答者を経営者／リスク管理部門（ＲＭ部門）／ＩＳ部門／ユーザ部門と分けても、すべての回答者がすべての質問項目について知っていることが少なくなる。つまり、ある質問項目について、回答者自身が社内で実施しているか否かを知らないため、「実施していない」と回答してしまうケースが想定される。この結果、平均点をとると実態よりも低い結果となってしまう。こういった事態を避けるために、回答者自身がよく知らない質問項目に対しては、＜D／K＞という回答を新設し、その質問項目について主管すべき回答者の回答が重視されるように変更した。

2）＜N／A（適用外項目）＞の追加

＜D／K＞が複数回答者のうち、その質問項目に該当しない回答者を除くために作られたのに対し、質問項目自体が該当しない場合、その質問項目を除くための＜N／A＞を追加した。たとえば、ある第４階層の質問項目に含まれる第５階層の質問で、その組織のシステム構成やユーザの業務特性により、第５階層のある質問項目が該当しない場合に適用される。たとえば、その企業のホームページの使い方が単なる情報提供で、利用者との取引を行うE-Commerceの機能を持っていない場合、関連する質問項目は＜N／A＞となる。

3）成熟度の判定基準

2001年度報告書でのレベル分けの考え方を、ＣＭＭやＣｏＢＩＴ－Ⅲ等の外部の基準と整合がとれるよう、表４－４のとおりとした。

表４－４．ＪＲＭＳの判定基準

| | |
|---|---|
| レベル３ | 組織内で標準が作られ、大体それに従って実施されている |
| レベル２ | 組織内で大体実施されているが、標準がない |
| レベル１ | 組織内で部分的にしか実施されていない |
| レベル０ | 組織内で全く意識されておらず、何もしていない |

4.2.2　成熟度モデルの説明

ＪＲＭＳでは、利用者が自組織のリスクマネジメントの現状を評価するために、成熟度モデルの考え方を取り入れている。成熟度モデルとは、ある業務プロセスの管理プラクティスについて、どの程度のレベルに達しているかを評価するモデルである。成熟度モデルの考え方には複数の標準があるが、その中でも、ＣＭＭはその歴史が古いことから一番よく使われている。これは、カーネギーメロン大学のソフトウェアエンジニアリングインスティテュートが提唱したモデルで、ソフトウェア開発のプロセスを対象に作られている。

ＣＭＭの成熟度モデルでは、各プロセスの成熟度レベルを表４－５のように定義している。

表４－５．ＣＭＭの成熟度モデル

| | | |
|---|---|---|
| レベル１ | 個別実施 | 開発方法論が存在せず、ほとんどコントロールされていない。プロセスが達成できたとしても、評価尺度が存在していないために認識されない。 |
| レベル２ | 反復可能 | プロジェクトの結果を妥当な精度で予測するのに十分な一連の作業とプロセスが定義されている。しかし、改善点を予めみつけたり、複数の選択を比較する手法は含まれていない。 |
| レベル３ | 定　義 | 開発プロセスは実装され、理解されている。評価尺度が用いられ、新たなテクノロジの実装の効果が予測できる程度に、プロセスの予測が可能である。 |
| レベル４ | 管　理 | プロセスが管理され発展することで、数量的、品質的な改善が可能である。それぞれの技術の実装は、全体的なアーキテクチャの一部となっている。 |
| レベル５ | 最　適 | 環境がプロセスを推進する、開発組織における理想的なレベル。プロセスの実行よりも、改善に注力される。 |

出典：ISO/IEC TR15504－4（http://www.imslab.co.jp/SSE-CMM/）

ＣＯＢＩＴ－Ⅲでは、ＣＭＭの成熟度モデルを参照しながら、開発プロセスに集中したＣＭＭに対し、対象を情報システムの全プロセスに拡大し、成熟度のレベルを定義している。また、ＣＭＭのレベル分けがレベル１～５となっているのに対し、レベル０を定義しているところが大きな違いである。

ＣＯＢＩＴ－Ⅲでの成熟度レベルは表４－６のように定義されている。

表４－６．ＣＯＢＩＴ－Ⅲの成熟度レベル

| | | |
|---|---|---|
| レベル０ | 未認識 | 組織として、当該プロセスの標準が必要なことすら認識されておらず、標準のプロセスも全くない。 |
| レベル１ | 初　期 | 組織として、当該プロセスの標準が必要なことは認識されているが、標準は確立されておらず、個人や場合によりその場限りの対応が行われている。プロセス全体についての組織的な対応はない。 |
| レベル２ | 反復可能 | ある作業を行う人たちが、同じ手続きを使うようになっている。しかし、標準手続きが公式的に教育・周知されてはおらず、個人任せになっている。各個人の知識に頼るところが多く、エラーも発生する。 |
| レベル３ | 定　義 | 手続きの標準化、文書化、教育・周知が行われている。しかし、標準のプロセスに従うかは個人任せなので逸脱が見られる。各手続きは、あまり洗練されてはおらず、既存のやり方を公式化したものである。 |
| レベル４ | 管　理 | 標準の手続きに従っているかをモニターし測定することが可能で、標準プロセスが有効でないときには是正措置を取ることができる。プロセスには絶えず改良が加えられ、グッドプラクティスが提供される。自動化ツールが部分的に利用されている。 |
| レベル５ | 最適化 | 継続的な改良と他組織の成熟度モデルを使ってプロセスはベストプラクティスのレベルまで改良されている。ＩＴは自動化されたワークフローに組み込まれ、品質や効率の改良のツールや企業の対応速度向上に役立っている。 |

出典：ＣＯＢＩＴ－Ⅲ（ISACA　2000.7）

また、ＮＩＳＴのSecurity Self-Assessment Guide for Information Technology Systemsでは、セキュリティに関わる17のトピックについて、表４－７のような成熟度のレベルを定義している。

表４－７．ＮＩＳＴの成熟度レベル

| | | |
|---|---|---|
| レベル１ | ポリシー | 管理目標が、セキュリティポリシーで定められている。 |
| レベル２ | 手続き | セキュリティコントロールの手続きが定められている。 |
| レベル３ | 実　施 | セキュリティコントロールの手続きが実施されている。 |
| レベル４ | テスト | セキュリティコントロールの手続きがテストされ、レビューされている。 |
| レベル５ | 統　合 | セキュリティコントロールの手続きが広範なプログラムに統合されている。 |

出典：National Institute Standard Technology (NIST)

### 4.2.3　成熟度モデルを使うメリット

適切なリスクマネジメントを実施するためには、リスクに関わる項目について経営者にわかりやすいように説明し、その理解を得て必要な投資に支援を得る必要がある。このためには、詳細な各項目ごとに実施の有無を＜Yes/No＞で判定し、それを大きな項目に集約し、より上位のレベルに適切なマッピングを行う必要がある。これにより、その項目について組織が継続的に改善をしていくための評価尺度が得られる。ＪＲＭＳの質問項目では、一番詳細な第５階層の質問項目に対しては、＜Yes/No＞で回答するが、第４階層は成熟度のレベルで回答する。これにより、各

質問項目についての回答が、各層ごとに集約されてレーダーチャートで状況が提示され、最終的に第一レベルの成熟度に反映される仕組みを作っている。

## 4.3 ＪＲＭＳの回答者

### 4.3.1 回答者の変更とその理由

前述のとおり、実証実験を踏まえてＪＲＭＳの構成を変えたが、変更点の一つとして「企業全体をみるリスクマネジメント」と「情報システムのリスクマネジメント」の章を明確に分けたことが挙げられる。2001 年度の委員会の検討段階では、組織の情報システム部門の責任者クラスであれば、企業全体のリスクマネジメントの状況も日常の業務遂行上の範囲で判断できる、また判断してほしいと考えていた。また経営者も組織のリスクマネジメントの実施への関与に加え、情報システムのリスクマネジメントの主要な要素については関与し判断できる、また判断してほしいと考えていた。

実証実験では、経営者層も情報システム部門も委員会の見解に従って各要素を回答していただき、十分な成果をあげた。経営者も質問をみて改めて情報システムリスクの管理点を認識し、情報システム部門も組織全体のリスクに目を向けることができた、など有意義な教育的効果があったとの回答を得ている。しかし、一般企業の現状をみると、組織の全社的なリスクマネジメントは普及が始まったばかりである。

このため、経営者や幹部職員が企業のリスクマネジメントに関与し、それに基づいて情報システムリスクにも関与するという双方向のリスク把握が可能な状態にはまだ至っていないと考え、組織全体のリスクマネジメントについては従来のＩＳ部門の代わりにリスクマネジメントの統轄部門を軸とするように変更した。また、経営者については情報システムリスクの各リスク分析やリスク対策の詳細については回答の対象からはずすこととした。

### 4.3.2 各項目別の回答者

ここで大項目別の回答者の整理を行うと表４－８のとおりとなる。

表４－８．大項目別回答者一覧

| 大項目 | | 経営者 | リスクマネジメント部門 | 情報システムリスクマネジメント組織 | ユーザ部門 |
|---|---|---|---|---|---|
| Ⅰ | 経営とリスクの関係 | ○ | ○ | 参画 | ○ |
| Ⅱ | ＪＲＭＳにおけるリスクマネジメント計画 | ○ | ○ | 参画 | ○ |
| Ⅲ | 情報システムのリスク分析 | | 参画 | ○ | ○ |
| Ⅳ | 情報システムにおけるリスク対策 | | 参画 | ○ | ○ |

表に示した「○」は必ず回答にあたり必須とする部門を表す。「参画」は必須ではないが必要に応じて責任者が回答者として参画することを表す。

実際の組織で全社のリスクマネジメントと情報システムリスクの相互理解がされている範囲に

もよるが、相互に参画できる人数が多い組織ほど、情報システムリスクが経営に直結していると考えられる。具体的に想定している各部門の回答者を表４－９に示す。

表４－９．層・部門別回答者一覧

| 層・部門 | 回答者 |
|---|---|
| 経営者層 | ・社長（ＣＥＯ、ＣＯＯ）<br>・リスクマネジメント担当役員（ＣＲＯ）<br>（リスクマネジメント担当が明確でない場合は経営企画担当役員や総務担当役員など）<br>・リスクマネジメント委員会のメンバー（役員）<br>財務担当役員（ＣＦＯ） |
| リスクマネジメント部門 | ・リスクマネジメント推進組織、保険部門の責任者、管理者、担当者<br><br>具体例：経営企画部、総務部の部課長、保険担当の部課長およびそれぞれの担当者などが該当 |
| 情報システムリスクマネジメント組織 | ・情報システム担当役員（ＣＩＯ）<br>・情報システムリスクマネジメント担当部門、情報システム企画・開発担当部門、情報システム運用およびセキュリティ担当部門の責任者、管理者、担当者<br><br>具体例：情報システム部長、システム開発課長、システム運用課長、セキュリティ管理課長およびそれぞれの担当者など |
| ユーザ部門 | ・適用業務の各アプリケーションの責任者およびその部門のリスク管理者、担当者<br><br>具体例：重要な業務のシステムのユーザ部門の部長、課長、担当者など |

ここでの留意点は、情報システムリスク担当部門に担当役員（ＣＩＯ）を含んでいることである。なぜなら、日本の実態から情報システム担当役員はリスク分析やリスク対策の詳細に関与することが求められることが多い、と判断したためである。

### 4.3.3　ＪＲＭＳ推進の責任者

従来のＪＲＭＳでは推進のための事務局は情報システム部門に設置することを想定しており、全社的なリスクマネジメントについても理想的にはまず情報システム部門の事務局で回答し、また、もし困難であればリスクマネジメント部門に委託することを想定していた。

今回の改訂で、基本的には全社的なリスクマネジメントの回答は事務局をリスクマネジメント部門が、また情報システムリスクについては情報システム部門が責任をもって回答することとした。このため組織全体にとり、「Ⅰ」から「Ⅳ」までの全体を統轄する最終責任者が不明確になる印象となるため、ここでこのＪＲＭＳの責任者を明確にしておく。

ＪＲＭＳの実施責任者は情報システム担当役員（ＣＩＯ）を想定している。手続き的には、ＪＲＭＳの推進の責任者は社長の委任により、情報システム担当役員（ＣＩＯ）が責任をもって実施することとなる。なお、ＣＩＯが明確に定められていない組織の場合は、経営者の中からふさ

わしい１名を社長が任命し、その役員が責任をもって実施する。

全社的なリスクマネジメントと情報システムのリスクマネジメント、双方の経営陣が理解してはじめて企業として情報システムリスクマネジメントが完遂できるのである。

#### 4.3.4　実践的なＪＲＭＳの推進組織

理想的には、「Ⅰ」、「Ⅱ」の全社のリスクマネジメントについてはＣＩＯからリスクマネジメント部門に指示を出し、回答の集計および集約を行う。また「Ⅲ」、「Ⅳ」の情報システムリスクについては情報システム部門に事務局を置き、回答の集計および集約を行う。回答者の選定にあたっては、全社のリスクマネジメントに対する回答者に情報システム部門の責任者・管理者から最低１名が参画し、また情報システムリスクに対する回答者に、リスクマネジメント部門の責任者・管理者から最低１名が参画することが望ましい。そして当然ながらＣＩＯは「Ⅰ」、「Ⅱ」、「Ⅲ」、「Ⅳ」のすべてに関与し回答する。

なお、全体の事務局は企業の実態にもよるが、ＣＩＯを実質補佐し、また情報システムリスクの具体的な実施を担う観点から、「Ⅰ」、「Ⅱ」の回答に情報セキュリティ部門が参画することができるのであれば、情報セキュリティ部門に全体の事務局を設置することが実践的である。

## 4.4　ＪＲＭＳとＩＳＭＳの相違点

#### 4.4.1　ＩＳＭＳの概要

ＪＲＭＳとＩＳＭＳの相違点についてあらためてその違いについて述べる。

ＩＳＭＳは情報セキュリティマネジメントシステムのことで「ISO17799」に準拠した制度であり、情報および情報システムのセキュリティに関して、規格に定められた項目に対して十分妥当な対策を実施しているかについて、第三者が認証する制度として一般的には認識されている。細かくいえば「ISO17799」およびそれに対応した「JIS X 5080」そのものは情報および情報システムのセキュリティに関するベストプラクティスを定めているだけで、認証制度ではない。一方「ISO17799」の基本となったイギリスの「BS7799 のパート２」は認証制度の仕組みである。また日本においては経済産業省の安対事業所認定制度という第三者認証制度を持っていたことから、この制度を移行することも含めてＩＳＭＳの認証制度を構築した。（「2.4　日本の動向」参照）

また「ISO17799」および「JIS X 5080」の内容として定められている要求事項として、①情報セキュリティポリシー、②セキュリティ推進組織、③情報資産の分類および脆弱性分析、④人的セキュリティ、⑤物理的環境的セキュリティ、⑥運用管理、⑦アクセス制御、⑧開発およびメンテナンス、⑨業務継続計画、⑩準拠、という 10 の大項目、また小項目の数ではこの内容をもとに作成される情報セキュリティ監査基準がわかりやすいが、約 1,000 項目からなる。旧来の各種の情報セキュリティの対策と比較すると、マネジメントシステムの名のとおり、経営の観点のチェック項目が含まれており、実際の認証にあたっては Plan－Do－Check－Action（ＰＤＣＡ）を繰り返し、情報セキュリティを維持改善できる体制を構築しているかどうかが重要視されている。

### 4.4.2　ＪＲＭＳの概要

ＪＲＭＳはＪＲＡＭから発展させた手法である。ＪＲＡＭ（JIPDEC Risk Analysis Method）は２つの要素があり、一つは事故分析から被害の定量的把握を行うことを目指したパート、もう一つが質問票による自己点検により情報システムの脆弱性を把握する手法のパートである。このうちＪＲＭＳは後者の質問票による脆弱性分析を行う手法を発展させたものである。質問票の内容はリスクマネジメントやセキュリティは経営者の関与が必要である、という経営学の危機管理およびリスクマネジメントの最新の知見を取り入れ、単なる情報システムリスク対策のチェックリストとはせずに、まず経営そのものにリスクマネジメント体制があるかどうかを重要視した。そのため経営のリスクマネジメントについて「JIS Q 2001」を参考に質問票を構成し、次に情報システムのリスクについてベストプラクティスとしての質問票を構成した。

ＪＲＭＳのＭＳはマネジメントシステムを意味し、「JIS Q 2001」や「ISO17799」のマネジメントシステムに関する要求事項をチェックポイントに取り入れたことを表している。

ところで、ＪＲＭＳはＪＲＡＭから発展させた手法であり、本来の目的もＪＲＡＭを認識すべきである。ＪＲＭＳの目的は質問項目を複数の人間が自己点検し、組織内の脆弱性をレーダーチャートの手法を用いて把握することである。その脆弱性の分析の際に経営者層、情報セキュリティ推進部門（またはリスクマネジメント推進部門）および情報システムのユーザ部門の３層から、どのように情報セキュリティが捕らえられているかについて比較する手法を用いているところに特徴がある。つまり、あるべき理想論からのギャップ、また経営者層、推進部門、ユーザ部門それぞれの認識のギャップを図るギャップ分析手法である。

### 4.4.3　ＩＳＭＳとＪＲＭＳの相違点

以上のように、ＩＳＭＳが情報および情報セキュリティの維持改善体制ができているかという第三者認証制度であるのに対し、ＪＲＭＳは組織のリスクマネジメント体制および情報セキュリティ体制の脆弱性把握のためのギャップ分析の手法であり、その目的とするところが異なっていることを認識することが必要である。一方、質問票の項目はともにマネジメントシステムを取り入れていること、情報セキュリティを扱っていることにより、情報セキュリティに関しては項目はほぼ同じ内容を網羅していることになる。

しいて着眼点の相違点をあげれば、ＩＳＭＳが情報システムに加えて情報にも着目していることがある。一方ＪＲＭＳは経営全般のリスクに着目していること、情報システムの企画、開発にも言及していることなどが挙げられる。

またＩＳＭＳは情報セキュリティのマネジメントの観点からセキュリティ事故の原因を明らかにする必要があるため、証拠保全について詳しいが、ＪＲＭＳはリスクの観点から特に触れていない。

## 4.5　まとめ

2002 年３月にＪＲＭＳを発表して以来、リスク対策検討委員会として委員会を 14 回開催し、ＪＲＭＳの構成ならびに質問項目（監査項目、ＪＲＭＳのリスク対策における実施基準の重視等）について検討を重ねた。「4.1　ＪＲＭＳ2003 の構成」において示した構成の変化・質問項目の見

直し作業の結果、ＪＲＭＳが経営関連の部分と情報システム部分の二つから構成されることになった。

とりわけ、レーダーチャートの作図ならびに回答結果の調整のためには、質問項目に対する回答の判定基準の設定はＪＲＭＳにとり重要な課題であった。質問項目が関係しない、または該当しない場合（Ｎ／Ａ）ならびに「知らない」場合（Ｄ／Ｋ）に関して、他の質問への回答結果の判定に影響が出ないようにするためには、見直しは不可欠であった。

さらに、回答における担当者については、経営の部分と情報システムの部分の二つから構成されることになったため、回答者および回答結果のとりまとめを行う責任者についても明確化することが必要であった。

これらが委員会における検討作業の成果である。ＪＲＭＳの修正・見直し作業により、ＪＲＭＳが情報システムに関するギャップ分析の手法として一段と精緻化され、組織におけるリスク対応にとり、有効性を高めることになったものと思われる。

しかしながら、システム環境の変化は著しい。ＪＲＭＳが現実のシステム環境に適合するため、ＪＲＭＳの利用組織において検証を重ね、常に質問項目の見直しを行うことが今後とも重要であるといえる。

# JRMS質問項目

| 大項目 | | 識別コード | 質問項目数 | | 該当項目数 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 第4階層の項目数 | 全項目数 | 経営者 | RM | IS | ユーザ |
| Ⅰ | 経営とリスクの関係 | | 9 | 21 | 8 | 20 | 0 | 18 |
| Ⅰ－1 | 経営環境とリスクマネジメント | 1－1－1－ 1 ～ 9 | 9 | 21 | 8 | 20 | | 18 |
| Ⅱ | JRMSにおけるリスクマネジメント計画 | | 79 | 237 | 48 | 236 | 0 | 212 |
| Ⅱ－1 | JRMSの計画 | 2－1－1－ 1 ～ 15 | 15 | 44 | 12 | 44 | | 40 |
| Ⅱ－2 | JRMSの実行組織 | 2－2－1－ 1 ～ 8 | 8 | 11 | 5 | 11 | | 7 |
| Ⅱ－3 | JRMSの維持 | 2－3－1－ 1 ～ 19 | 19 | 31 | 6 | 30 | | 23 |
| Ⅱ－4 | JRMSのリスク分析 | 2－4－1－ 1 ～ 27 | 27 | 125 | 19 | 125 | | 125 |
| Ⅱ－5 | JRMSのリスク対策 | 2－5－1－ 1 ～ 10 | 10 | 26 | 6 | 26 | | 17 |
| Ⅲ | 情報システムのリスク分析 | | 54 | 152 | 0 | 0 | 152 | 87 |
| Ⅲ－1 | 情報セキュリティポリシーのリスク分析 | 3－1－1－ 1 ～ 10 | 10 | 26 | 0 | | 26 | 13 |
| Ⅲ－2 | 情報システムのリスク分析 | | 19 | 64 | 0 | 0 | 64 | 44 |
| | (1)情報システムのリスク分析 | 3－2－1－ 1 ～ 7 | 7 | 36 | 0 | | 36 | 22 |
| | (2)システム開発 | 3－2－2－ 1 ～ 5 | 5 | 15 | 0 | | 15 | 13 |
| | (3)システム運用 | 3－2－3－ 1 ～ 3 | 3 | 6 | 0 | | 6 | 3 |
| | (4)アウトソーシング | 3－2－4－ 1 ～ 4 | 4 | 7 | 0 | | 7 | 6 |
| Ⅲ－3 | 情報システムの個別リスク分析 | | 25 | 62 | 0 | 0 | 62 | 30 |
| | (1)不正アクセス・コンピュータウイルス関連 | 3－3－1－ 1 ～ 12 | 12 | 23 | 0 | | 23 | 7 |
| | (2)災害 | 3－3－2－ 1 ～ 6 | 6 | 21 | 0 | | 21 | 19 |
| | (3)障害 | 3－3－3－ 1 ～ 7 | 7 | 18 | 0 | | 18 | 4 |
| Ⅳ | 情報システムにおけるリスク対策 | | 245 | 594 | 0 | 0 | 592 | 285 |
| Ⅳ－1 | リスク対策における情報セキュリティ | 4－1－1－ 1 ～ 29 | 29 | 91 | 0 | | 89 | 73 |
| Ⅳ－2 | 情報システムのリスク対策 | | 94 | 167 | 0 | 0 | 167 | 104 |
| | (1)情報システム総合企画 | 4－2－1－ 1 ～ 29 | 29 | 36 | 0 | | 36 | 29 |
| | (2)システム開発 | 4－2－2－ 1 ～ 22 | 22 | 61 | 0 | | 61 | 20 |
| | (3)システム運用 | 4－2－3－ 1 ～ 7 | 7 | 23 | 0 | | 23 | 9 |
| | (4)アウトソーシング | 4－2－4－ 1 ～ 36 | 36 | 36 | 0 | | 36 | 36 |
| | (5)システム監査 | 4－2－5－ 1 ～ 6 | 6 | 11 | 0 | | 11 | 10 |
| Ⅳ－3 | 不正アクセス・コンピュータウイルス関連 | | 60 | 151 | 0 | 0 | 151 | 59 |
| | (1)コンピュータ犯罪 | 4－3－1－ 1 ～ 9 | 9 | 22 | 0 | | 22 | 13 |
| | (2)不正アクセス | 4－3－2－ 1 ～ 19 | 19 | 53 | 0 | | 53 | 23 |
| | (3)コンピュータウイルス | 4－3－3－ 1 ～ 10 | 10 | 22 | 0 | | 22 | 13 |
| | (4)E－Commerce | 4－3－4－ 1 ～ 11 | 11 | 31 | 0 | | 31 | 6 |
| | (5)電子メール | 4－3－5－ 1 ～ 11 | 11 | 23 | 0 | | 23 | 4 |
| Ⅳ－4 | 災害対策 | 4－4－1－ 1 ～ 28 | 28 | 57 | 0 | | 57 | 8 |
| Ⅳ－5 | 障害対策 | 4－5－1－ 1 ～ 12 | 12 | 37 | 0 | | 37 | 12 |
| Ⅳ－6 | その他関連項目 | 4－6－1－ 1 ～ 7 | 7 | 18 | 0 | | 18 | 18 |
| Ⅳ－7 | バックアップ | 4－7－1－ 1 ～ 10 | 10 | 41 | 0 | | 41 | 2 |
| Ⅳ－8 | 緊急時対策 | 4－8－1－ 1 ～ 5 | 5 | 32 | 0 | | 32 | 9 |
| 計 | | | 387 | 1,004 | 56 | 256 | 744 | 602 |

キーワード一覧

網掛け：大項目KW/標準：第4階層KW/斜体字：第5階層KW

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅰ．経営とリスクの関係 | Ⅰ－1．経営環境とリスクマネジメント | 1．経営者の関心 | 2．リスクマネジメントポリシー | 3．リスクマネジメントポリシーのフレームワーク | 4．リスクマネジメントポリシーの監査 | 5．リスクマネジメントポリシーの周知 | | | | |
| | | 経営者の関心 | 全社的なリスクマネジメントポリシー | 基本目的 | 監査 | 周知 | | | | |
| | | | *最高経営者の承認* | 経営への脅威 | *内部監査* | | | | | |
| | | | *経営理念との整合* | *守るべき対象* | *外部監査* | | | | | |
| | | | | *役割・責任* | | | | | | |
| | | | | *課題の明確化* | | | | | | |
| | | | | *社会的責任の明確化* | | | | | | |
| | | | | *マイナス情報の吸い上げ* | | | | | | |
| | | | | *緊急事態発生時対応* | | | | | | |
| | | | | *コンプライアンス違反* | | | | | | |
| | | | | 責任部門 | | | | | | |
| | | | | 実施基準 | | | | | | |
| | | | | *フィードバックループ* | | | | | | |
| | | | | 行動指針 | | | | | | |
| Ⅱ．JRMSにおけるリスクマネジメント計画 | Ⅱ－1．JRMSの計画 | 1．経営理念と計画 | 2．管理体制の組織化 | 3．管理目標 | 4．目標脅威 | 5．分析 | 6．対策 | 7．緊急時対応 | 8．リスクマネジメント計画の周知 | |
| | | 経営理念 | 管理体制 | 管理目標 | 目標脅威 | 分析方法 | リスク対策への反映 | 緊急時対応 | 周知 | |
| | | 保護対象 | *リスク分析責任者* | *物理的資産* | *物理的資産* | *費用対効果分析* | 対策策定方法 | *事故* | | |
| | | | *リスク対策責任者* | *情報資産* | *情報資産* | *ハザード分析* | 対策実施基準 | *自然災害* | | |
| | | | *リスクファイナンス責任者* | *経済的損失* | *経済的損失* | *ギャップ分析* | 経営者の承認 | *商品瑕疵、サービス欠陥* | | |
| | | | 基本目的 | *機会損失* | *機会損失* | | | *製品、サービス供給停止* | | |
| | | | 対策実施の責任権限 | *企業信用、ブランド価値* | *企業信用、ブランド価値* | | | *企業信用、ブランド価値* | | |
| | | | 意思決定プロセス | *人的資産* | *人的資産* | | | *人的資産* | | |
| | | | | *コンプライアンス* | *コンプライアンス違反* | | | *コンプライアンス違反* | | |
| | | | | | *サイバーテロ* | | | *サイバーテロ* | | |
| | Ⅱ－2．JRMSの実行組織 | 1．全社的リスクマネジメント組織 | 2．情報システムリスクマネジメント組織 | 3．ユーザの組織 | | | | | | |
| | | リスクマネジメント担当役員の任命 | 情報システムリスク管理体制 | 適用業務別オーナー | | | | | | |
| | | リスクマネジメント推進体制 | *情報システムリスク管理者* | ユーザ部門リスク担当責任者 | | | | | | |
| | | リスクマネジメント担当者の役割権限 | *情報システム運用管理責任者* | | | | | | | |
| | | 情報システムリスクマネジメント担当者の役割権限 | 情報セキュリティ対策推進組織 | | | | | | | |
| | | | *情報システム情報セキュリティ管理者* | | | | | | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅱ. JRMSにおけるリスクマネジメント計画 | Ⅱ－3. JRMSの維持 | 1. 評価 | 2. 是正改善 | 3. 監査 | 4. 監視 | 5. 文書化 | 6. リスクコミュニケーション | 7. 教育の承認 | 8. 教育の実施 | 9. 経営者のレビュー |
| | | パフォーマンス評価 | 是正改善 | リスクマネジメントシステム監査 | 変化の監視 | 基準の文書化 | リスクコミュニケーションの実施 | 経営者の教育承認 | 経営者の教育 | リスクマネジメントシステムレビュー |
| | | *パフォーマンス評価基準* | *是正改善行動採択基準* | *内部監査* | 監視手段 | リスクマネジメント文書管理 | *リスクコミュニケーション手段* | *経営者層の教育訓練計画* | 情報システム部門の教育 | |
| | | *パフォーマンス監視* | *フィードバックループ機能* | *外部監査* | | リスク変化の記録 | リスク情報開示 | *情報システム部門の教育訓練計画* | ユーザ部門の教育 | |
| | | 有効性評価 | *是正改善状況の点検* | | | 実績記録 | | *ユーザ部門の教育訓練計画* | | |
| | | | *是正改善の有効性評価* | | | | | 教育の位置づけ | | |
| | | | ボトルネックの排除 | | | | | | | |
| | Ⅱ-4. JRMSNのリスク分析 | 1. リスク分析の仕組み | 2. リスク分析の体制 | 3. リスク分析の実施 | 4. リスク分析（災害） | 5. リスク分析（事故） | 6. リスク分析（情報システム） | 7. リスク分析（経営） | 8. リスク分析（政治・経済・社会） | |
| | | JRMSのリスク分析の実施 | 変化を含めた社内体制 | リスク洗い出し | 自然災害 | 事故 | 情報システム障害 | 製品トラブル | 政治的トラブル | |
| | | 未実施の場合の問題状況の認識 | 対応優先順位 | *洗い出し実施基準* | *地震・津波・噴火* | *火災・爆発* | *停止* | *製品瑕疵* | *法律の制定・制度改革・税制改革* | |
| | | 関連情報提供システム | フィードバック | *日常的な洗い出し* | *台風・高潮* | *設備故障* | *電子メール使用不可による影響* | *製造物責任* | *国際社会の圧力（外圧）* | |
| | | 保護対象リスク分析 | 分析の予算・スタッフ | *特定部門からの要請による洗い出し* | *水災・洪水* | *停電* | *誤作動* | *リコール・欠陥製品* | *貿易制限・通商問題* | |
| | | | | 頻度算定 | *竜巻・風災* | *交通事故* | *改ざん* | *苦情処理対応トラブル* | *戦争・内乱* | |
| | | | | *頻度算定実施基準* | *落雷* | *人的損失* | *破壊* | 知的財産権侵害 | *政変・革命* | |
| | | | | 影響度算定 | *雪害* | *労災事故* | *情報漏洩* | *特許紛争* | 経済的トラブル | |
| | | | | *影響度算定実施基準* | *雹害* | *建設中の事故* | セキュリティホール | *実用新案侵害* | *経済危機・景気変動* | |
| | | | | リスク評価 | *天候不良・異常気象* | *運送中の事故* | *ネットワーク障害* | *商標権侵害* | *株価・為替・金利・地価変動* | |
| | | | | *リスク評価基準* | | *盗難・海賊* | | *著作権侵害* | *原料・資材高騰* | |
| | | | | | | *放射能汚染・放射能漏れ* | | 環境問題 | 社会的トラブル | |
| | | | | | | *有害微生物、細菌漏洩・バイオハザード* | | 環境規制強化 | *市場ニーズの変化* | |
| | | | | | | 漏水 | | *環境賠償責任・環境規則違反* | *社会的影響* | |
| | | | | | | *動物害* | | *環境汚染・油濁事故* | *競合・顧客のグローバル化* | |
| | | | | | | | | *廃棄物処理・リサイクル* | *情報技術革新* | |
| | | | | | | | | 雇用トラブル | *テロ・暴動* | |
| | | | | | | | | *差別* | *誘拐・人質* | |
| | | | | | | | | *使用者責任* | *暴力団・総会屋・脅迫* | |
| | | | | | | | | *セクシャルハラスメント* | *インターネットによる批判・中傷* | |
| | | | | | | | | *労働争議・ストライキ・デモ* | *マスコミによる批判・中傷* | |
| | | | | | | | | *伝染病* | *風評* | |
| | | | | | | | | *役員・スタッフの不正、不法行為* | *不買運動・消費者運動* | |
| | | | | | | | | *職場暴力* | | |
| | | | | | | | | *集団離職* | | |
| | | | | | | | | *外国人不法就労* | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅱ. JRMSにおけるリスクマネジメント計画 | Ⅱ-4. JRMSNのリスク分析 | | | | | | | 海外従業員の雇用調整 | | |
| | | | | | | | | 海外駐在員の安全 | | |
| | | | | | | | | 従業員の高齢化 | | |
| | | | | | | | | 法務上のトラブル | | |
| | | | | | | | | 商法違反・カルテル | | |
| | | | | | | | | 独禁法違反 | | |
| | | | | | | | | 役員賠償責任 | | |
| | | | | | | | | インサイダー取引 | | |
| | | | | | | | | プライバシー侵害 | | |
| | | | | | | | | 資産運用トラブル | | |
| | | | | | | | | デリバティブ失敗 | | |
| | | | | | | | | 不良債権・貸し倒れ | | |
| | | | | | | | | 信用トラブル | | |
| | | | | | | | | 情報管理の不備・顧客情報漏洩 | | |
| | | | | | | | | 不正取引・詐欺 | | |
| | | | | | | | | 経営全般トラブル | | |
| | | | | | | | | 企業倫理 | | |
| | | | | | | | | 取引先倒産 | | |
| | | | | | | | | 格付下落・金融支援の停止 | | |
| | | | | | | | | 経営者の死亡 | | |
| | | | | | | | | 乱脈経営 | | |
| | | | | | | | | 不適切な宣伝・広告 | | |
| | | | | | | | | 不測事態発生時の対応 | | |
| | | | | | | | | 社内不正 | | |
| | | | | | | | | 共謀犯罪 | | |
| | | | | | | | | 役員のスキャンダル | | |
| | | | | | | | | 経営者・従業員の不正・犯罪 | | |
| | | | | | | | | 共謀情報漏れ | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅱ. JRMSにおけるリスクマネジメント計画 | Ⅱ－5. JRMSのリスク対策 | 1. リスク対策の体制 | 2. 財務的対応 | 3. リスク対応のための組み合わせ | 4. テロ | 5. 人名損失 | | | | |
| | | 事業の継続性 | 保険リスク | リスクファイナンス成果評価基準 | テロ | 人命損失対策の決定 | | | | |
| | | 対策の明確化 | *コンピュータ総合保険* | | *テロ対策* | *人命損失による影響* | | | | |
| | | *自然災害* | *利益保険* | | *脅迫・トラブル* | *避難訓練* | | | | |
| | | *事故* | *賠償責任保険* | | | | | | | |
| | | *経営* | *コンピュータ機器保険* | | | | | | | |
| | | *政治・経済・社会* | *カントリーリスク* | | | | | | | |
| | | 管理不能リスクの明確化 | *保有リスク* | | | | | | | |
| | | *財務的対応* | リスクファイナンス見直し | | | | | | | |
| | | *リスク対応のための各種方法組み合わせ* | 実施関連部所間の協議 | | | | | | | |
| | | リスクファイナンス | | | | | | | | |
| Ⅲ. 情報システムのリスク分析 | Ⅲ－1. 情報セキュリティポリシーのリスク分析 | 1. 情報セキュリティの経営からの視点 | 2. 情報セキュリティポリシーの対象 | 3. 特筆する情報リスク | 4. 時間分析 | 5. 情報リスク洗い出し実施基準 | | | | |
| | | 経営の視点からの分析 | リスク分析の対象 | 基幹システム情報漏洩（情報） | 機能停止 | 情報リスク洗い出し実施基準 | | | | |
| | | | *災害* | ホームページ（情報） | | | | | | |
| | | | *障害* | システミックリスク | | | | | | |
| | | | *不正アクセス* | 基幹システムダウン | | | | | | |
| | | | *偽造・不正使用リスク* | | | | | | | |
| | | | *コンピュータウイルス* | | | | | | | |
| | | | *ネットワーク障害* | | | | | | | |
| | | | *アウトソーシングのリスク* | | | | | | | |
| | | | *SLA* | | | | | | | |
| | | | 緊急時対応 | | | | | | | |
| | | | *機密漏洩* | | | | | | | |
| | | | *不正アクセス* | | | | | | | |
| | | | *コンピュータウイルス* | | | | | | | |
| | | | *ネットワーク障害* | | | | | | | |
| | | | *災害* | | | | | | | |
| | | | *障害* | | | | | | | |
| | | | *緊急時対応* | | | | | | | |
| | | | *ファシリティ移動* | | | | | | | |
| | | | 情報セキュリティ推進組織内容 | | | | | | | |
| | | | *監査内容* | | | | | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅲ. 情報システムのリスク分析 | Ⅲ－2. 情報システムのリスク分析 | 3－2－(1)情報システムのリスク分析 | 1. IT戦略のリスク分析 | 2. 情報資産リスク | 3. システム不全 | 4. 適用業務責任・権限 | 5. 適用業務とリスクマネジメント | | | | |
| | | | IT戦略のリスク分析 | 情報資産リスク | 機能不全 | 適用業務責任・権限 | 情報システム適用業務 | | | | |
| | | | *情報システムの重要度測定* | *重要性ランキング* | *ネットワーク* | *企画業務* | 設計時の前提 | | | | |
| | | | *情報の重要度測定* | *オーナーの明確化* | *誤作動* | *開発業務* | | | | | |
| | | | *業務への影響* | *機密度ランク* | *犯罪* | *運用業務* | | | | | |
| | | | *E-Commerce* | *可用性維持* | *対応ミス* | *保守業務* | | | | | |
| | | | *情報リスクと経営存続* | *複数人によるリスク分析* | *質低下* | *予算業務* | | | | | |
| | | | | 人的リスク | *安全性・機密保持の悪化* | *その他機能分野* | | | | | |
| | | | | *改ざんリスク* | *変化への対応性欠如* | | | | | | |
| | | | | *破棄* | | | | | | | |
| | | | | *盗難* | | | | | | | |
| | | | | *物理的侵入* | | | | | | | |
| | | | | *物理的攻撃* | | | | | | | |
| | | | | *倒産* | | | | | | | |
| | | 3－2－(2)システム開発 | 1. プロジェクトリスク | 2. ライフサイクル | 3. 開発管理 | 4. 運用テスト | | | | | |
| | | | プロジェクトリスク | ライフサイクル | 開発管理 | 運用テスト結果 | | | | | |
| | | | *企画段階* | | *スタッフのスキルの妥当性* | *稼働開始による障害発生* | | | | | |
| | | | *技術面* | | *コンプライアンス* | *運用テスト結果* | | | | | |
| | | | *ビジネス面* | | *開発環境* | | | | | | |
| | | | *組織面* | | *ソフトウェアのサポート切れ* | | | | | | |
| | | | | | *ソフトウェアのバージョンアップ* | | | | | | |
| | | 3－2－(3)システム運用 | 1. システム運用 | 2. 運用管理 | 3. キャパシティ管理 | | | | | | |
| | | | 円滑運用 | ファイル管理 | キャパシティ管理 | | | | | | |
| | | | | *ライブラリ管理* | | | | | | | |
| | | | | *バックアップ* | | | | | | | |
| | | | | *適用業務管理* | | | | | | | |
| | | 3－2－(4)アウトソーシング | 1. アウトソーサの決定 | 2. 役割分担 | 3. 守秘義務 | | | | | | |
| | | | アウトソーサの選定手続き | 契約内容 | 守秘義務 | | | | | | |
| | | | | *責任分担* | 再委託時の守秘義務 | | | | | | |
| | | | | *作業内容* | | | | | | | |
| | | | | *変更管理* | | | | | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅲ. 情報システムのリスク分析 | Ⅲ－3. 情報システムの個別リスク分析 | 3－3－(1)不正アクセス・コンピュータウイルス関連 | 1. コンピュータ犯罪のリスク | 2. 不正アクセスのリスク | 3. コンピュータウイルスのリスク | 4. 電子メールのリスク | 5. ネットワークのリスク | | | | |
| | | | 経営に与える影響 | モバイル機器盗難 | コンピュータウイルス被害・復旧コスト | コンピュータウイルス誤配 | ネットワークの大規模なダウン | | | | |
| | | | 内部犯罪による信頼への影響 | インターネット経由内部犯罪 | コンピュータウイルス被害による機会損失 | | | | | | |
| | | | 経営者・従業員の意識 | ネッティングリスク | 感染の影響 | | | | | | |
| | | | 盗聴による影響 | 妨害行為 | 取引先への影響 | | | | | | |
| | | | 脅迫による影響 | | 株価への影響 | | | | | | |
| | | | 改ざん | | 損害賠償請求 | | | | | | |
| | | | 破壊 | | ベンダ緊急時対応の遅れ | | | | | | |
| | | | 情報漏洩 | | アンチウイルス更新遅れ | | | | | | |
| | | | | | 定期検診以上の莫迦 | | | | | | |
| | | 3－3－(2)災害 | 1. 管理 | 2. 災害 | 3. 事故 | 4. 人的災害 | 5. 委託先リスクの可能性 | | | | |
| | | | 情報システムへの影響 | 自然災害 | 事故 | 人的災害 | 委託先リスクの可能性 | | | | |
| | | | 災害復旧手順 | 地震・津波・噴火 | 火災・爆発 | 戦争・動乱・暴動による影響 | | | | | |
| | | | | 台風・高潮 | 停電 | 人的リスクの可能性 | | | | | |
| | | | | 水災・洪水 | 人的損失 | | | | | | |
| | | | | 竜巻・風災 | 漏水 | | | | | | |
| | | | | 落雷 | 動物害 | | | | | | |
| | | | | 雪害 | | | | | | | |
| | | | | 雹害 | | | | | | | |
| | | | | 天候不良・異常気象 | | | | | | | |
| | | 3－3－(3)障害 | 1. 管理 | 2. ハードウェア障害 | 3. ソフトウェア障害 | 4. 運用ミス障害 | | | | | |
| | | | 情報システムへの影響 | ハードウェア障害 | ソフトウェア障害 | 運用ミス障害 | | | | | |
| | | | 復旧手順 | ネットワーク(WAN)障害 | OS、ライセンスプログラム障害 | バックアップ不備 | | | | | |
| | | | | サーバ障害 | アプリケーションプログラム停止 | ソフトウェア更新手続きミス | | | | | |
| | | | | ISPサービス機能障害 | アプリケーションプログラム誤処理 | 人的リスクの可能性 | | | | | |
| | | | | 端末機器障害 | 端末機器障害 | | | | | | |
| | | | | 停電 | その他ソフトウェア障害 | | | | | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－1. リスク対策における情報セキュリティ | 1. 情報セキュリティポリシー | 2. 情報セキュリティポリシーに基づく実施基準 | 3. 情報資産インベントリ | 4. スタッフ | 5. 情報セキュリティ個別対策 | 6. 自社ホームページ承認 | 7. 教育内容 | | |
| | | 情報セキュリティポリシー | 情報セキュリティポリシーに基づく実施基準 | 情報資産目録 | 情報セキュリティ管理・担当者 | 操作と業務処理手順 | 自社ホームページ承認 | 情報システム部門の教育内容 | | |
| | | | *情報システム総合企画* | *劣化媒体の排除* | *スタッフ* | 出張、移動中の実施基準 | *掲載許可* | *緊急事態対応* | | |
| | | | *システム開発* | *重要計算の取扱いと重要装置の仕様* | *業務ローテーション* | 携帯端末利用 | *コンテンツの知的財産権* | *誤作動対応* | | |
| | | | *システム運用* | 機密度ランク | *外部のコンサルタント* | *ユーザ認証、アクセス管理* | ホームページ記載内容のチェック | *システム停止対応* | | |
| | | | *アウトソーシング* | | | *携帯端末紛失連絡体制* | コンテンツ侵害への手続き | *システム侵入対応* | | |
| | | | *システム監査* | | | 情報システム利用手続き | *営業機密漏洩チェック* | ユーザ部門の教育内容 | | |
| | | | *コンピュータ犯罪* | | | リスク管理文書化 | | *緊急事態対応* | | |
| | | | *不正アクセス* | | | データ、媒体利用 | | | | |
| | | | *コンピュータウイルス* | | | ログ確認 | | | | |
| | | | *E-Commerce* | | | *アクセスログ権限* | | | | |
| | | | *電子メール* | | | *機密情報ログ* | | | | |
| | | | *災害対策* | | | プログラムソースライブラリ管理 | | | | |
| | | | *障害対策* | | | 基幹システムの国際利用 | | | | |
| | | | *その他関連項目* | | | 個人情報保護 | | | | |
| | | | *バックアップ* | | | プロバイダ選定基準 | | | | |
| | | | *緊急時対策* | | | | | | | |
| | | | リスクマネジメントシステム計画との整合性 | | | | | | | |
| | | | *企業特性* | | | | | | | |
| | | | *論理的な構築* | | | | | | | |
| | | | *評価リスト* | | | | | | | |
| | | | *緊急事態復旧計画* | | | | | | | |
| | | | *ISO15408との整合性* | | | | | | | |
| | | | *ISO17799との整合性* | | | | | | | |
| | | | 実施基準での禁止事項 | | | | | | | |
| | | | *市販ソフトのコピー使用* | | | | | | | |
| | | | *データ・プログラムの無断使用* | | | | | | | |
| | | | *機密情報搾取行為* | | | | | | | |
| | | | *覗き見* | | | | | | | |
| | | | *コンピュータ私用利用* | | | | | | | |
| | | | *コンピュータウイルス伝染行為* | | | | | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－1. リスク対策における情報セキュリティ | | | *不正侵入行為* | | | | | | | |
| | | | | *WWWの私用利用* | | | | | | | |
| | | | | *データ不正入力* | | | | | | | |
| | | | | *私用電子メール使用* | | | | | | | |
| | | | | *ファイルの覗き見行為* | | | | | | | |
| | | | | *仕事以外のファイルの覗き見行為* | | | | | | | |
| | | | | *他人のID無断使用* | | | | | | | |
| | | | | *接続されたマシンの無断操作* | | | | | | | |
| | | | | *時間外でのコンピュータ私用利用* | | | | | | | |
| | | | | *顧客情報の売却* | | | | | | | |
| | | | | *ホームページによる誹謗中傷行為* | | | | | | | |
| | | | | *電子掲示板による誹謗中傷行為* | | | | | | | |
| | | | | *動作障害行為* | | | | | | | |
| | | | | *プログラム・データ改ざん* | | | | | | | |
| | | | | *無許可情報の開示行為* | | | | | | | |
| | | | | *スパムメール発信行為* | | | | | | | |
| | | | | *社会秩序を乱す情報提供* | | | | | | | |
| | | | | コンプライアンス | | | | | | | |
| | | | | 罰則規程 | | | | | | | |
| | | | | 情報オーナーの責任 | | | | | | | |
| | | | | 自己点検システム・監査システム | | | | | | | |
| | | | | 実施基準の定期的見直し | | | | | | | |
| | | | | 企業内教育 | | | | | | | |
| | | | | 情報セキュリティポリシーの徹底 | | | | | | | |
| | Ⅳ－2. 情報システムのリスク対策 | 4－2－(1)情報システム総合企画 | 1. 実施基準 | 2. IT戦略 | 3. IT計画 | 4. 組織体制・機能 | 5. スタッフ | 6. 財務 | 7. 管理(文書化を含む) | 8. モニタリング | |
| | | | 情報システム総合企画 | 経営戦略との整合 | IT戦略とITインフラ計画 | 指揮命令系統 | 人事計画 | 投資収益方針 | 全社データ管理 | 規制監視 | |
| | | | | 標準ステップ | ITインフラ計画 | セキュリティ機能 | スキル | 投資決定方法 | 全社データ標準化 | 是正措置 | |
| | | | | 外部規制 | 導入計画 | *インターナルコントロール機能* | プロジェクト管理スキル | *短期的影響の想定* | 全社データ所有者の識別 | | |
| | | | | | | *品質管理機能* | 品質管理教育 | *長期的影響の想定* | 管理工程分割 | | |
| | | | | | | 決裁権限 | | *他部門への影響の想定* | 工程ごとの品質基準 | | |
| | | | | | | リスク別担当部門 | | *ビジネス上の採算* | ライセンス管理 | | |
| | | | | | | | | 予定利益 | プロジェクト管理標準 | | |
| | | | | | | | | IT資産管理目録 | *方法論* | | |
| | | | | | | | | 関連費用識別 | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－2. 情報システムのリスク対策 | 4－2－(2)システム開発 | 1. 実施基準 | 2. プロジェクト管理 | 3. システム要件定義 | 4. プログラム開発 | 5. テストデータ | 6. 運用テスト | 7. 変更管理 | | |
| | | | システム開発 | システム開発方法論 | セキュリティ基準の遵守 | 開発環境 | テストデータ | テスト仕様書の内容 | 管理責任者 | | |
| | | | 決裁実施基準 | 作業内容と成果物 | 要件の反映 | 機密保持のクラス分け | テストの機密保持規定 | 運用テストの結果 | バージョンアップ手続き | | |
| | | | 開発に応じた決裁 | 技法／ツール | SLA合意 | プログラムライブラリへのアクセス管理 | 保護データの排除 | 導入の妥当性 | 管理方針 | | |
| | | | システム調達のライフサイクルにおけるセキュリティ | 判定基準 | システム要件の反映 | 高機密プログラムの保管 | 本番データ使用時の保護対策 | システム性能 | 非常時の実施基準 | | |
| | | | 調達 | 進捗管理手続き | システム構成要素の入手可能性 | 設計文書保管 | 本番データとの分離 | 操作性確認 | バックアップ・他所保管の実施基準 | | |
| | | | 不正防止・機密保護基準 | | | 不正ソフトの混入対策 | | 異常時バックアップ対応 | 区分によるバージョンアップ | | |
| | | | 破棄基準 | | | コンプライアンス | | | 変更管理 | | |
| | | | 品質管理 | | | 知的財産権放棄・契約の要求事項 | | | 識別のための体系 | | |
| | | | 要員 | | | 個人情報保護 | | | ネーミングルール | | |
| | | | 職務定義 | | | 暗号輸出入管理 | | | 高機密プログラム保管 | | |
| | | | 職務分離 | | | 各国法規遵守 | | | レビュー検証 | | |
| | | | 情報セキュリティ保持の役割・責任 | | | | | | レビュー内容の文書化 | | |
| | | | 機密保持合意 | | | | | | 管理責任者の承認 | | |
| | | | | | | | | | 作業とレビューの分離 | | |
| | | | | | | | | | アクセスの職務分離 | | |
| | | | | | | | | | 配布先でのバージョン管理 | | |
| | | 4－2－(3)システム運用 | 1. 実施基準 | 2. システム運用 | 3. モニタリング機能 | 4. 管理機能 | 5. 復旧時間 | | | | |
| | | | システム運用 | システム運用実施 | 記録・状況把握 | ファイル世代管理 | SLA | | | | |
| | | | システム運用計画 | 定期的見直し | 記録・監視 | ライブラリ管理 | | | | | |
| | | | | 構成管理 | 報告体制 | 障害管理 | | | | | |
| | | | | 運用マニュアル | モニタリング | 適用業務管理方針 | | | | | |
| | | | | スケジュール運用確認 | アプリケーションシステム | | | | | | |
| | | | | 運用手順 | 共用データ | | | | | | |
| | | | | データの適切性 | サーバ・クライアント端末 | | | | | | |
| | | | | スキルの妥当性 | ネットワーク | | | | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－2. 情報システムのリスク対策 | 4－2－(4)アウトソーシング関連リスク対策 | 1 実施基準 | 2 目的 | 3 役割分担 | 4 プロジェクト管理 | 5 アウトソーサ管理 | 6 契約 | 7 知的財産権 | 8 セキュリティ上の留意点 | |
| | | | アウトソーシング | TCC | 責任分担 | プロジェクト管理手法 | 選定評価基準 | 委託契約ルール | 再委託 | 委託先情報セキュリティ | |
| | | | | コスト削減 | 役割分担 | 共通開発方法論 | SLA | 賠償上限 | 知的財産権 | 委託先情報セキュリティ実施状況 | |
| | | | | スリム化 | 受託者の作業内容 | 外注委託のレビュー | ペナルティ | 海外委託 | 知的財産権侵害 | 委託先情報セキュリティ遵守 | |
| | | | | 関連技術の安価利用 | 委託者の作業内容 | 会議体 | 運用障害時対応 | 開発納期延期 | | 秘密保持 | |
| | | | | コスト削減 | | | ソフトウェア障害時対応 | ソフトウェア瑕疵担保 | | 再委託時の秘密保持 | |
| | | | | | | | 品質管理 | 契約監査 | | | |
| | | | | | | | | 受託先監査 | | | |
| | | | | | | | | 変更手続き | | | |
| | | 4－2－(5)監査 | 1 実施基準 | 2 監査 | 3 監査基準 | | | | | | |
| | | | システム監査 | 重要性の認識 | 監査基準 | | | | | | |
| | | | | *システム監査の実施* | | | | | | | |
| | | | | *内部監査* | | | | | | | |
| | | | | *外部監査* | | | | | | | |
| | | | | *監査人の選任* | | | | | | | |
| | | | | *リスクマネジメント責任者と監査人の位置づけ* | | | | | | | |
| | | | | 報告先 | | | | | | | |
| | | | | 勧告のフォロー | | | | | | | |
| | | | | 監査未実施 | | | | | | | |
| | Ⅳ－3. 不正アクセス | Ⅳ－3－(1)コンピュータ犯罪 | 1 実施基準 | 2 内部犯罪の防止 | 3 データ保護対策 | 4 盗聴対策 | 5 緊急時対応 | | | | |
| | | | コンピュータ犯罪 | パスワードの変更 | データ保護対策 | 盗聴対策 | ネットワーク対策 | | | | |
| | | | *内部犯罪対策* | *内部犯罪の定義* | *暗号化* | *録音機器持込管理* | 外部機関への相談 | | | | |
| | | | *個人利用禁止* | ネットワーク機器 | *デジタル署名* | *携帯電話持込* | 証拠保全 | | | | |
| | | | *不正使用対策* | 個人使用システム | *暗合鍵* | *PDA* | | | | | |
| | | | | | *セキュリティホール対策* | *無線LAN* | | | | | |
| | | | | | | *電磁波漏れ* | | | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－3. 不正アクセス | Ⅳ－3－(2)不正アクセス | 1. 実施基準 | 2. アクセス管理 | 3. 物理的アクセス対策 | 4. 論理的アクセス対策 | 5. ネットワーク中のデータ保護 | 6. 外部アクセスからのデータ保護 | 7. 不正検出 | 8. 緊急時対応 | |
| | | | 不正アクセス | アクセス管理 | 不正侵入防止 | 重要なデータ保護対策 | ネットワークの不正アクセス対策 | 移動体内臓データ保護 | アクセスログ確認 | 緊急対処方法 | |
| | | | *アクセス権、ID／パスワード付与、チェック体制* | *不正アクセス防止* | *ネットワーク機器の不正防止* | *暗号* | *暗号化転送* | *接続方式* | *プロトコル* | IPAへの届出 | |
| | | | *物理的アクセス対策* | *データ保護* | *物理的破壊対策* | *デジタル署名* | ファイアウォール | *認証* | *ログ保存* | JPCERT/CCへの相談 | |
| | | | *論理的アクセス対策* | *暗号利用* | | *暗号鍵管理* | *DMZ* | *ネットワークサービス* | *ログ確認* | 外部機関への相談 | |
| | | | *外部からのアクセス* | ID付与 | | 個人認証 | *ファイアウォールレイアウト* | *ソーシャルエンジニアリング対策* | | | |
| | | | *緊急時対策* | *ID・パスワード付与のレビュー* | | *入退室* | *重要データ保存管理* | | | | |
| | | | | *不正入手* | | *システム個人認証* | *ログ記録機能* | | | | |
| | | | | *アクセス権付与チェック・レビュー* | | 中継地回避の実施基準 | *ログ自動分析ツール* | | | | |
| | | | | 機密度・アクセス制限 | | 中継地懸念とログ分析 | *検知機能* | | | | |
| | | | | 職務分離 | | | | | | | |
| | | | | インターネット利用 | | | | | | | |
| | | | | 教育、訓練 | | | | | | | |
| | | | | *不正アクセス対策教育* | | | | | | | |
| | | 4－3－(3)コンピュータウイルス | 1. 実施基準 | 2. ウイルス検出・駆除 | 3. 教育・訓練 | 4. ウイルス感染対策 | 5. 事後対策 | | | | |
| | | | コンピュータウイルス対策 | ウイルス防止ソフト | 教育・訓練 | 緊急連絡体制 | 事後対策 | | | | |
| | | | *感染時の緊急時・事後対策* | *ウイルス検出・駆除* | *システム管理者の教育・訓練* | *影響判断* | *感染情報* | | | | |
| | | | | | ユーザの教育・訓練 | *情報収集* | *通知* | | | | |
| | | | | | | *感染ルート* | *対策強化* | | | | |
| | | | | | | 感染の緊急時対策 | *復旧対策* | | | | |
| | | | | | | ウイルスの感染防止 | *再発防止対策* | | | | |
| | | | | | | 伝染防止対策 | *組織の共有化* | | | | |
| | | | | | | | IPAへの届出 | | | | |
| | | 4－3－(4)E-Commerce | 1. 実施基準 | 2. プライバシー保護 | 3. 不良客情報管理 | 4. データ保護対策 | 5. ネットワーク機器対応 | 6. インターネット接続管理 | 7. 電子的証拠 | | |
| | | | E-Commerce | プライバシー保護対策 | 不払い、不良客情報管理 | 電子商取引時のデータ保護対策 | ネットワーク機器、サーバの信頼性 | インターネット接続の規制 | デジタル署名 | | |
| | | | *個人情報保護対策* | *コンプライアンスプログラム* | *不良客情報入手* | インターネットからの攻撃 | ネットワーク機器、サーバの性能 | インターネット接続機器管理 | 時刻証明 | | |
| | | | *データ保護対策* | *プライバシーマーク取得* | | *DOS攻撃対策* | | *ファイアウォール管理* | | | |
| | | | *インターネット利用対策* | *クッキー対策* | | *アタック対策* | | *IDS* | | | |
| | | | *電子取引規定* | | | *セキュリティホール対策* | | *DNS管理* | | | |
| | | | | | | *コンピュータウイルス対策* | | *暗号* | | | |
| | | | | | | *スパムメール対策* | | *暗号利用に関する通知* | | | |
| | | | | | | 改ざん対策 | | *不正行為監視* | | | |

| カテゴリ | | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－3. 不正アクセス | 4－3－(5)電子メール | 1. 実施基準 | 2. メールサーバ管理 | 3. ネットワーク機器管理 | 4. デジタル署名 | 5. 悪質メール対策 | 6. 転送エラー対策 | | | |
| | | | 電子メール利用対策 | メールサーバのデータ保護対策 | ネットワーク機器、サーバの信頼性 | デジタル署名 | 添付ファイル | 転送エラー | | | |
| | | | *ユーザ利用* | メールサーバへの攻撃 | ネットワーク機器、サーバの性能 | | スクリプト | | | | |
| | | | *サーバ管理* | *DOS攻撃対策* | インターネット接続機器管理 | | 不正メール対策 | | | | |
| | | | *インターネット利用* | *不正アクセス対策* | *ファイアウォール管理* | | | | | | |
| | | | | *セキュリティホール対策* | *DNS管理* | | | | | | |
| | | | | *コンピュータウイルス対策* | *暗号* | | | | | | |
| | | | | *不正メール転送* | *不正行為監視* | | | | | | |
| | Ⅳ－4. 災害対策 | | 1. 実施基準 | 2. 管理 | 3. 防火対策 | 4. 耐震対策 | 5. 水害対策 | | | | |
| | | | 災害対策 | 経営者の決定 | 防火壁 | フリーアクセス耐震補強 | コンピュータ室 | | | | |
| | | | *自然災害対策* | 災害復旧レベル | *コンピュータ室* | コンピュータ機器の固定 | 上げ床 | | | | |
| | | | *事故災害対策* | *事業再開* | *データ保管場所* | 転倒防止 | 防水堤・ピット | | | | |
| | | | *人的災害対策* | *災害復旧レベル* | *ネットワーク設備室* | 機器・ラックの固定 | 漏水検知機 | | | | |
| | | | | *改善レベル* | *コンピュータ設置場所* | テープ落下防止策 | 排水口 | | | | |
| | | | | 是正措置 | 自動消火装置 | 機器の落下防止策 | 水落下防止策 | | | | |
| | | | | 避難対策 | *コンピュータ室* | 電源設備 | 吹き込み対策 | | | | |
| | | | | | *データ保管場所* | | 防水シート | | | | |
| | | | | | *ネットワーク設備室* | | 電源設備 | | | | |
| | | | | | *コンピュータ設置場所* | | | | | | |
| | | | | | 区画放出対応消火システム | | | | | | |
| | | | | | *コンピュータ室* | | | | | | |
| | | | | | *データ保管場所* | | | | | | |
| | | | | | *ネットワーク設備室* | | | | | | |
| | | | | | 消火器 | | | | | | |
| | | | | | *コンピュータ室* | | | | | | |
| | | | | | *データ保管場所* | | | | | | |
| | | | | | *ネットワーク設備室* | | | | | | |
| | | | | | *コンピュータ設置場所* | | | | | | |
| | | | | | 消火栓 | | | | | | |
| | | | | | *コンピュータ室* | | | | | | |
| | | | | | *データ保管場所* | | | | | | |
| | | | | | *ネットワーク設備室* | | | | | | |
| | | | | | *コンピュータ設置場所* | | | | | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－4. 災害対策 | | | 遮断装置 | | | | | | |
| | | | | コンピュータ室 | | | | | | |
| | | | | データ保管場所 | | | | | | |
| | | | | ネットワーク設備室 | | | | | | |
| | | | | コンピュータ設置場所 | | | | | | |
| | | | | 2方向非常口 | | | | | | |
| | Ⅳ－5. 障害対策 | 1. 実施基準 | 2. 管理 | 3. 手続き | 4. 情報システム | 5. ユーティリティ | 6. ネットワーク対策 | 7. 復旧 | | |
| | | 障害対策 | 障害対策 | ソフトウェア更新手続き | ディスク障害対策 | 施設障害対策 | 回線障害対策 | 復旧レベル | | |
| | | ハードウェア障害対策 | 運用監視機能 | 最終テスト結果確認 | | 適用業務優先順位 | 避雷針 | 代替手段 | | |
| | | ソフトウェア障害対策 | 障害検出機能 | 更進記録整備 | | 無停電装置 | ネットワーク障害対策 | 是正措置 | | |
| | | 運用ミス障害 | 縮退運転機能 | 記録内容 | | 無停電装置テスト | | | | |
| | | | 代替運転機能 | 更新確認 | | 供給能力 | | | | |
| | | | 回復機能 | ソフトウェア更新 | | 空調設備の多重化 | | | | |
| | | | サービスレベル | 障害管理票 | | 水冷 | | | | |
| | | | ポリシーとの整合性 | 変更後障害 | | | | | | |
| | | | 管理責任者の承認 | | | | | | | |
| | | | トランザクション量 | | | | | | | |
| | | | トランザクション量の測定 | | | | | | | |
| | Ⅳ－6. その他関連項目 | 1. 実施基準 | 2. サービス提供 | 3. ユーザ間トラブル | 4. 苦情処理対応 | 5. 危機管理計画徹底 | 6. 危機管理計画徹底 | | | |
| | | その他関連項目 | 会員規約 | ユーザ間トラブルの決定 | 苦情処理対応の決定 | 危機管理計画の内外関係者への徹底 | 危機管理計画の内外関係者への徹底 | | | |
| | | 経営リスク | 規約違反 | ユーザ間トラブル対策 | 苦情処理対応策 | 物的資産喪失・破壊 | 物的資産喪失・破壊 | | | |
| | | 政治・経済・社会リスク | 通信の秘密保護教育 | 法的責任・事後対応 | 苦情処理対応マネジメントシステム | 情報資産喪失・破壊 | 情報資産喪失・破壊 | | | |
| | | テロ対策 | | 法的責任・事後対応対象 | | その他資産喪失・破壊 | その他資産喪失・破壊 | | | |
| | Ⅳ－7. バックアップ | 1. 実施基準 | 2. 二重化対策 | 3. ファイルのバックアップ | 4. ネットワーク対策 | 5. 予備サイト | | | | |
| | | バックアップ対策 | 二重化対策 | プログラムバックアップ | 代替回線 | 予備サイト設置 | | | | |
| | | | 交換機、チャネル | 実施方法 | 代替機 | 同一室内のバックアップ用コンピュータ | | | | |
| | | | 機器 | 遠隔地保管 | 手作業による代替手段 | 同一建物内のバックアップ用コンピュータ | | | | |
| | | | LAN | 同一サイト内保管 | | バックアップセンタ | | | | |
| | | | WAN | OSファイルバックアップ | | 遠隔地バックアップセンタ | | | | |
| | | | 切り替えテスト | 実施方法 | | バックアップサービス業者 | | | | |
| | | | | 遠隔地保管 | | 相互バックアップ契約 | | | | |
| | | | | 同一サイト内保管 | | | | | | |
| | | | | データファイルバックアップ | | | | | | |

| カテゴリ | | キーワード一覧 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Ⅳ. 情報システムにおけるリスク対策 | Ⅳ－7. バックアップ | | | 実施方法 | | | | | | |
| | | | | 遠隔地ミラーデータ | | | | | | |
| | | | | 遠隔地保管 | | | | | | |
| | | | | 同一サイト内保管 | | | | | | |
| | | | | 保存期間 | | | | | | |
| | | | | バックアップ頻度 | | | | | | |
| | | | | DBファイルバックアップ | | | | | | |
| | | | | 実施方法 | | | | | | |
| | | | | 遠隔地ミラーDB | | | | | | |
| | | | | 遠隔地保管 | | | | | | |
| | | | | 同一サイト内保管 | | | | | | |
| | | | | ボリューム | | | | | | |
| | | | | 災害時用同一ディスク保有 | | | | | | |
| | | | | ログバックアップ | | | | | | |
| | | | | ログの分別化 | | | | | | |
| | Ⅳ－8. 緊急時対策 | 1. 実施基準 | 2. 事前対応 | 3. 緊急時対応手続き | 4. 復旧計画 | | | | | |
| | | 緊急時対策 | 緊急時対応の訓練 | 緊急時対応手続きの明確化 | 復旧計画 | | | | | |
| | | 障害発生 | | 緊急連絡網 | 復旧オーナ、管理者の選定 | | | | | |
| | | 機密漏洩対策 | | 緊急時対応体制 | 代替手段 | | | | | |
| | | 不正アクセス | | 代替対応手順 | 計画維持・テストのスケジュール化 | | | | | |
| | | マクロウイルス | | 障害解決のフローチャート化 | | | | | | |
| | | 自然災害 | | 教育訓練計画 | | | | | | |
| | | 倒産 | | 対策本部 | | | | | | |
| | | 法令侵害 | | 判定基準 | | | | | | |
| | | バックアップ | | 緊急事態宣言 | | | | | | |
| | | ファシリティ移動 | | 情報資産 | | | | | | |
| | | | | 不審・異常ログ発見時の通報手順 | | | | | | |
| | | | | バックアップ手順 | | | | | | |
| | | | | 危機障害発生時の適用業務優先順位 | | | | | | |
| | | | | 障害切り分け | | | | | | |
| | | | | 障害発生アラーム | | | | | | |
| | | | | 障害管理票 | | | | | | |
| | | | | 定期的評価、是正改善 | | | | | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| 経営とリスク | 経営とリスク | Ⅰ．経営とリスクの関係 | | | | | |
| 経営環境とリスクマネジメント | 経営環境とリスクマネジメント | Ⅰ－1．経営環境とリスクマネジメント | | | | | |
| 1．経営者の関心 | 経営者の関心 | 1- 1- 1- 1 | Q 経営者は役員会において経営に関するリスクについて議論をしていますか？ | ● | | | |
| 2．リスクマネジメントポリシー | 全社的なリスクマネジメントポリシー | 1- 1- 1- 2 | Q 全社的なリスクマネジメントポリシー(方針)を有していますか？ | ● | ● | ● | |
| | 最高経営者の承認 | 1- 1- 1- 2- 1 | Q リスクマネジメントポリシーは、最高経営者の承認のもと全社的に策定されていますか？ | ● | ● | | |
| | 経営理念との整合 | 1- 1- 1- 2- 2 | Q リスクマネジメントポリシーは、貴社の経営理念に基づいて定めていますか？ | | ● | | |
| 3．リスクマネジメントポリシーのフレームワーク | 基本目的 | 1- 1- 1- 3 | Q リスクマネジメントポリシーは、基本目的が明確に設定されていますか？ | ● | ● | ● | |
| | 経営への脅威 | 1- 1- 1- 4 | Q リスクマネジメントポリシーでは、経営を脅かすリスクが明確にされていますか？ | ● | ● | ● | |
| | 守るべき対象 | 1- 1- 1- 4- 1 | Q リスクマネジメントポリシーでは、組織として守るべき対象を明確にしていますか？ | | ● | ● | |
| | 役割・責任 | 1- 1- 1- 4- 2 | Q リスクマネジメントポリシーでは、守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？ | | ● | ● | |
| | 課題の明確化 | 1- 1- 1- 4- 3 | Q リスクマネジメントポリシーでは、組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？ | | ● | ● | |
| | 社会的責任の明確化 | 1- 1- 1- 4- 4 | Q リスクマネジメントポリシーでは、課題にリスクに対する社会的責任をも含んでいますか？ | | ● | ● | |
| | マイナス情報の吸い上げ | 1- 1- 1- 4- 5 | Q リスクマネジメントポリシーでは、経営にとってのマイナス情報を吸い上げる機能がありますか？ | ● | ● | ● | |
| | 緊急事態発生時対応 | 1- 1- 1- 4- 6 | Q リスクマネジメントポリシーでは、緊急事態発生時の役員、スタッフ、担当者の役割が定められていますか？ | | ● | ● | |
| | コンプライアンス違反 | 1- 1- 1- 4- 7 | Q リスクマネジメントポリシーでは、コンプライアンス違反に対する処置を明示していますか？ | | ● | ● | |
| | 責任部門 | 1- 1- 1- 5 | Q リスクマネジメントポリシーでは、リスクに関する責任部門が明記されていますか？ | ● | ● | ● | |
| | 実施基準 | 1- 1- 1- 6 | Q リスクマネジメントポリシーでは、実施基準が明確ですか？ | | ● | ● | |
| | フィードバックループ | 1- 1- 1- 6- 1 | Q リスクマネジメントポリシーが有効に機能するようフィードバックループ構成になっていますか？ | | ● | ● | |
| | 行動指針 | 1- 1- 1- 7 | Q リスクマネジメントポリシーでは、組織としてなすべき行動指針が明確にされていますか？ | ● | ● | ● | |
| 4．リスクマネジメントポリシーの監査 | 監査 | 1- 1- 1- 8 | Q リスクマネジメントポリシーでは、監査の実施が明確に定められていますか？ | | ● | ● | |
| | 内部監査 | 1- 1- 1- 8- 1 | Q リスクマネジメントポリシーでは、内部監査の実施を明記していますか？ | | ● | ● | |
| | 外部監査 | 1- 1- 1- 8- 2 | Q リスクマネジメントポリシーでは、外部監査の実施を明記していますか？ | | ● | ● | |
| 5．リスクマネジメントポリシーの周知 | 周知 | 1- 1- 1- 9 | Q リスクマネジメントポリシーを関係者に周知していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| JRMS計画 | JRMS計画 | Ⅱ－1. JRMSの計画 | | | | | |
| 1. 経営理念と計画 | 経営理念 | 2- 1- 1- 1 | Q リスクマネジメント計画では、経営理念を明確に反映していますか？ | ● | ● | | |
| | 保護対象 | 2- 1- 1- 2 | Q リスクマネジメント計画では、護るべき対象を明確にしていますか？ | ● | ● | ● | |
| 2. 管理体制の組織化 | 管理体制 | 2- 1- 1- 3 | Q リスクマネジメント計画では、リスク管理の体制が定義されていますか？ | ● | ● | ● | |
| | リスク分析責任者 | 2- 1- 1- 3- 1 | Q リスク分析の責任者が定められていますか？ | | ● | ● | |
| | リスク対策責任者 | 2- 1- 1- 3- 2 | Q リスク対策の責任者が定められていますか？ | | ● | ● | |
| | リスクファイナンス責任者 | 2- 1- 1- 3- 3 | Q リスクファイナンスに関する責任者が定められていますか？ | | ● | ● | |
| | 基本目的 | 2- 1- 1- 4 | Q リスクマネジメント計画ではリスクマネジメントにおける基本的な目的がわかりやすく示されていますか？ | ● | ● | ● | |
| | 対策実施の責任権限 | 2- 1- 1- 5 | Q リスクマネジメント計画ではリスク対策の実施にあたって、責任権限が明確ですか？ | | ● | ● | |
| | 意思決定プロセス | 2- 1- 1- 6 | Q リスクマネジメント計画では意思決定プロセスが明確ですか？ | | ● | ● | |
| 3. 管理目標 | 管理目標 | 2- 1- 1- 7 | Q リスクマネジメント計画ではリスクマネジメントの管理目標を具体的に明示していますか？ | ● | ● | ● | |
| | 物理的資産 | 2- 1- 1- 7- 1 | Q 物理的資産の管理目標を具体的に明示していますか？ | | ● | ● | |
| | 情報資産 | 2- 1- 1- 7- 2 | Q 情報資産(無形)の管理目標を具体的に明示していますか？ | | ● | ● | |
| | 経済的損失 | 2- 1- 1- 7- 3 | Q 経済的損失の管理目標を具体的に明示していますか？ | | ● | ● | |
| | 機会損失 | 2- 1- 1- 7- 4 | Q 機会損失の管理目標を具体的に明示していますか？ | | ● | ● | |
| | 企業信用、ブランド価値 | 2- 1- 1- 7- 5 | Q 企業の信用やブランド価値の管理目標を具体的に明示していますか？ | | ● | ● | |
| | 人的資産 | 2- 1- 1- 7- 6 | Q 人的資産の管理目標を具体的に明示していますか？ | | ● | ● | |
| | コンプライアンス | 2- 1- 1- 7- 7 | Q コンプライアンスの管理目標を具体的に明示していますか？ | ● | ● | ● | |
| 4. 目標脅威 | 目標脅威 | 2- 1- 1- 8 | Q 具体的な目標を脅かすリスクやハザードについて情報の視点から分析を行っていますか？ | ● | ● | ● | |
| | 物理的資産 | 2- 1- 1- 8- 1 | Q 物理的資産を脅かすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | 情報資産 | 2- 1- 1- 8- 2 | Q 情報資産(無形)を脅かすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | 経済的損失 | 2- 1- 1- 8- 3 | Q 経済的損失をもたらすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | 機会損失 | 2- 1- 1- 8- 4 | Q 機会損失をもたらすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | 企業信用、ブランド価値 | 2- 1- 1- 8- 5 | Q 企業の信用やブランド価値を脅かすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | 人的資産 | 2- 1- 1- 8- 6 | Q 人的資産を脅かすリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| | コンプライアンス違反 | 2- 1- 1- 8- 7 | Q コンプライアンス違反によるリスクについて情報の視点から分析を行っていますか？ | ● | ● | ● | |
| | サイバーテロ | 2- 1- 1- 8- 8 | Q サイバーテロ(踏み台攻撃を含む)によるリスクやハザードについて情報の視点から分析を行っていますか？ | | ● | ● | |
| 5. 分析 | 分析方法 | 2- 1- 1- 9 | Q リスク分析の方法は明確ですか？ | | ● | ● | |
| | 費用対効果分析 | 2- 1- 1- 9- 1 | Q 費用対効果分析の方法は明確ですか？ | | ● | | |
| | ハザード分析 | 2- 1- 1- 9- 2 | Q ハザード分析の方法は明確ですか？ | | ● | | |
| | ギャップ分析 | 2- 1- 1- 9- 3 | Q ギャップ分析の方法は明確ですか？ | | ● | | |
| 6. 対策 | リスク対策への反映 | 2- 1- 1- 10 | Q リスク分析の結果をリスク対策に反映させていますか？ | | ● | ● | |
| | 対策策定方法 | 2- 1- 1- 11 | Q リスク対策の策定方法は明確ですか？ | | ● | ● | |
| | 対策実施基準 | 2- 1- 1- 12 | Q リスク対策のための実施基準を有していますか？ | | ● | ● | |
| | 経営者の承認 | 2- 1- 1- 13 | Q リスク対策の採用につき経営者が最終承認していますか？ | ● | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| JRMS計画 | JRMS計画 | Ⅱ－1. JRMSの計画 | | | | | |
| 7. 緊急時対応 | 緊急時対応 | 2- 1- 1- 14 | Q リスクマネジメント計画では緊急時対応について明記していますか？ | ● | ● | ● | |
| | 事故 | 2- 1- 1- 14- 1 | Q 事故に対する緊急時対応を明記していますか？ | | ● | ● | |
| | 自然災害 | 2- 1- 1- 14- 2 | Q 災害に対する緊急時対応を明記していますか？ | | ● | ● | |
| | 商品瑕疵、サービス欠陥 | 2- 1- 1- 14- 3 | Q 商品の瑕疵やサービスの欠陥に対する緊急時対応を明記していますか？ | | ● | ● | |
| | 製品、サービス供給停止 | 2- 1- 1- 14- 4 | Q 製品やサービスの供給が停止した場合の緊急時対応を明記していますか？ | | ● | ● | |
| | 企業信用、ブランド価値 | 2- 1- 1- 14- 5 | Q 企業の信用やブランド価値が損なわれた場合の緊急時対応を明記していますか？ | | ● | ● | |
| | 人的資産 | 2- 1- 1- 14- 6 | Q 人的資産が損なわれた場合の緊急時対応を明記していますか？ | | ● | ● | |
| | コンプライアンス違反 | 2- 1- 1- 14- 7 | Q コンプライアンス違反を犯した場合の緊急時対応を明記していますか？ | ● | ● | ● | |
| | サイバーテロ | 2- 1- 1- 14- 8 | Q サイバーテロ（踏み台攻撃を含む）への緊急時対応を明記していますか？ | | ● | ● | |
| 8. リスクマネジメント計画の周知 | 周知 | 2- 1- 1- 15 | Q リスクマネジメント計画を関係者に周知させていますか？ | ● | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| 実行組織 | 実行組織 | Ⅱ－2. JRMSの実行組織 | | | | | |
| 1. 全社的リスクマネジメント組織 | リスクマネジメント担当役員の任命 | 2- 2- 1- 1 | Q リスクマネジメントのための担当役員は最高経営者により任命されていますか？ | ● | ● | | |
| | リスクマネジメント推進体制 | 2- 2- 1- 2 | Q リスクマネジメントシステム推進のための体制がありますか？ | ● | ● | ● | |
| | リスクマネジメント担当者の役割権限 | 2- 2- 1- 3 | Q リスクマネジメント担当者の役割権限が明確ですか？ | ● | ● | ● | |
| | 情報システムリスクマネジメント担当者の役割権限 | 2- 2- 1- 4 | Q 情報システムリスクマネジメント担当者が任命されていますか？ | ● | ● | ● | |
| 2. 情報システムリスクマネジメント組織 | 情報システムリスク管理体制 | 2- 2- 1- 5 | Q 情報システムのリスク管理体制がありますか？ | ● | ● | ● | |
| | 情報システムリスク管理者 | 2- 2- 1- 5- 1 | Q 情報システムのリスク管理者がいますか？ | | ● | | |
| | 情報システム運用管理責任者 | 2- 2- 1- 5- 2 | Q 情報システムの運用管理責任者がいますか？ | | ● | | |
| | 情報セキュリティ対策推進組織 | 2- 2- 1- 6 | Q 情報システムの情報セキュリティ対策推進組織がありますか？ | | ● | ● | |
| | 情報システム情報セキュリティ管理者 | 2- 2- 1- 6- 1 | Q 情報システムの情報セキュリティの管理者がいますか？ | | ● | | |
| 3. ユーザの組織 | 適用業務別オーナー | 2- 2- 1- 7 | Q 情報システムの適用業務に関するユーザ側のオーナーは明確ですか？ | | ● | ● | |
| | ユーザ部門リスク担当責任者 | 2- 2- 1- 8 | Q ユーザ部門の適用業務に対するリスク担当責任者がいますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| 維持 | 維持 | Ⅱ-3. JRMSの維持 | | | | | |
| 1. 評価 | パフォーマンス評価 | 2- 3- 1- 1 | Q リスクマネジメントシステムに関するパフォーマンス評価を実施していますか？ | ● | ● | | |
| | パフォーマンス評価基準 | 2- 3- 1- 1- 1 | Q リスクマネジメントシステムの実施に関するパフォーマンス評価基準がありますか？ | | ● | | |
| | パフォーマンス監視 | 2- 3- 1- 1- 2 | Q リスクマネジメントシステムの実施に関するパフォーマンス監視を行っていますか？ | | ● | | |
| | 有効性評価 | 2- 3- 1- 2 | Q リスクマネジメントシステムの有効性評価を行っていますか？ | | ● | ● | |
| 2. 是正改善 | 是正改善 | 2- 3- 1- 3 | Q リスクマネジメントシステムに関して是正・改善を実施していますか？ | ● | ● | ● | |
| | 是正改善行動採択基準 | 2- 3- 1- 3- 1 | Q リスク対応のため、是正改善行動を採択する基準がありますか？ | | ● | ● | |
| | フィードバックループ機能 | 2- 3- 1- 3- 2 | Q 是正改善を繰り返し反映させる(フィードバックループ)機能はありますか？ | | ● | ● | |
| | 是正改善状況の点検 | 2- 3- 1- 3- 3 | Q 是正改善の状況を点検していますか？ | | ● | | |
| | 是正改善の有効性評価 | 2- 3- 1- 3- 4 | Q 是正改善の実施後に有効性評価を行っていますか？ | | ● | ● | |
| | ボトルネックの排除 | 2- 3- 1- 4 | Q リスクマネジメントシステムの実施にあたり、ボトルネックの排除を行っていますか？ | | ● | ● | |
| 3. 監査 | リスクマネジメントシステム監査 | 2- 3- 1- 5 | Q リスクマネジメントシステムの監査を実施していますか？ | ● | ● | ● | |
| | 内部監査 | 2- 3- 1- 5- 1 | Q 内部監査によるリスクマネジメントシステム監査を実施していますか？ | | ● | ● | |
| | 外部監査 | 2- 3- 1- 5- 2 | Q 外部監査によるリスクマネジメントシステム監査を実施していますか？ | | ● | ● | |
| 4. 監視 | 変化の監視 | 2- 3- 1- 6 | Q 発見したリスクの変化を監視していますか？ | | ● | ● | |
| | 監視手段 | 2- 3- 1- 7 | Q リスクの変化を監視する手段を持っていますか？ | | ● | ● | |
| 5. 文書化 | 基準の文書化 | 2- 3- 1- 8 | Q リスクマネジメントシステムに用いる実施基準は文書化されていますか？ | | ● | ● | |
| | リスクマネジメント文書管理 | 2- 3- 1- 9 | Q リスクマネジメントシステム実施に関する文書管理を行っていますか？ | | ● | ● | |
| | リスク変化の記録 | 2- 3- 1- 10 | Q リスクの変化に関する記録を行っていますか？ | | ● | ● | |
| | 実績記録 | 2- 3- 1- 11 | Q リスクマネジメントの実施に関する記録を行っていますか？ | | ● | ● | |
| 6. リスクコミュニケーション | リスクコミュニケーションの実施 | 2- 3- 1- 12 | Q リスクコミュニケーションを実施していますか？ | | ● | ● | |
| | リスクコミュニケーション手段 | 2- 3- 1- 12- 1 | Q リスクコミュニケーション手段(電子メール、説明会等)を明確にしていますか？ | | ● | ● | |
| | リスク情報開示 | 2- 3- 1- 13 | Q リスク情報の開示に関する実施基準を策定していますか？ | | ● | ● | |
| 7. 教育の承認 | 経営者の教育承認 | 2- 3- 1- 14 | Q 経営者はリスクマネジメントに関する教育訓練計画を承認していますか？ | ● | ● | ● | |
| | 経営者層の教育訓練計画 | 2- 3- 1- 14- 1 | Q 経営者層に対するリスクマネジメントに関する教育訓練計画を承認していますか？ | | ● | | |
| | 情報システム部門の教育訓練計画 | 2- 3- 1- 14- 2 | Q 情報システム部門に対するリスクマネジメントに関する教育訓練計画を承認していますか？ | | ● | | |
| | ユーザ部門の教育訓練計画 | 2- 3- 1- 14- 3 | Q ユーザ部門に対するリスクマネジメントに関する教育訓練計画を承認していますか？ | | | ● | |
| | 教育の位置づけ | 2- 3- 1- 15 | Q 組織維持のためリスクマネジメントに関する教育の位置づけは明確ですか？ | | ● | ● | |
| 8. 教育の実施 | 経営者の教育 | 2- 3- 1- 16 | Q 経営者層に対するリスクマネジメント教育訓練を行っていますか？ | ● | ● | | |
| | 情報システム部門の教育 | 2- 3- 1- 17 | Q システム部門に対するリスクマネジメント教育訓練を行っていますか？ | | ● | | |
| | ユーザ部門の教育 | 2- 3- 1- 18 | Q ユーザ部門に対するリスクマネジメント教育訓練を行っていますか？ | | ● | ● | |
| 9. 経営者のレビュー | リスクマネジメントシステムレビュー | 2- 3- 1- 19 | Q 最高経営者によるリスクマネジメントシステムのレビューを行っていますか？ | ● | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| リスク分析 | リスク分析 | Ⅱ-4. JRMSのリスク分析 | | | | | |
| 1. リスク分析の仕組み | JRMSリスク分析の実施 | 2- 4- 1- 1 | Q リスク分析(発見・算定・評価)の実施についてリスクマネジメント計画上明確にしていますか？ | ● | ● | ● | |
| | 未実施の場合の問題状況の認識 | 2- 4- 1- 2 | Q リスク分析を実施していない場合の問題を認識していますか？ | ● | ● | ● | |
| | 関連情報提供システム | 2- 4- 1- 3 | Q リスク関連情報をリスク分析担当者に提供する仕組みが構築されていますか？ | ● | ● | ● | |
| | 保護対象リスク分析 | 2- 4- 1- 4 | Q 明確にされた守るべき対象についてリスクを分析していますか？ | | ● | ● | |
| 2. リスク分析の体制 | 変化を含めた社内体制 | 2- 4- 1- 5 | Q 内外の経営環境の変化を含めたリスク環境の動きを捉える社内体制を有していますか？ | ● | ● | ● | |
| | 対応優先順位 | 2- 4- 1- 6 | Q リスク評価を行い、リスク対応の優先順位を確定していますか？ | | ● | ● | |
| | フィードバック | 2- 4- 1- 7 | Q リスク発見・評価の見直しを繰り返し反映する機能をもっていますか？ | | ● | ● | |
| | 分析の予算・スタッフ | 2- 4- 1- 8 | Q 予算・スタッフをリスク分析のため適切に導入していますか？ | | ● | ● | |
| 3. リスク分析の実施 | リスク洗い出し | 2- 4- 1- 9 | Q 定期的にリスクを洗い出していますか？ | | ● | ● | |
| | 洗い出し実施基準 | 2- 4- 1- 9- 1 | Q リスクをもれなく洗い出す実施基準を有していますか？ | | ● | ● | |
| | 日常的な洗い出し | 2- 4- 1- 9- 2 | Q 経営環境の変化から生じるリスクを日常的に洗い出していますか？ | | ● | ● | |
| | 特定部門からの要請による洗い出し | 2- 4- 1- 9- 3 | Q 特定機能部門からの要請によりリスクの洗い出しを行っていますか？ | | ● | ● | |
| | 頻度算定 | 2- 4- 1- 10 | Q リスク頻度を算定していますか？ | | ● | ● | |
| | 頻度算定実施基準 | 2- 4- 1- 10- 1 | Q リスク頻度を算定する実施基準を用意していますか？ | | ● | ● | |
| | 影響度算定 | 2- 4- 1- 11 | Q リスク影響度を算定していますか？ | | ● | ● | |
| | 影響度算定実施基準 | 2- 4- 1- 11- 1 | Q リスク影響度を算定する実施基準を用意していますか？ | | ● | ● | |
| | リスク評価 | 2- 4- 1- 12 | Q リスク評価を実施していますか？ | | ● | ● | |
| | リスク評価基準 | 2- 4- 1- 12- 1 | Q リスク評価基準を用意していますか？ | | ● | ● | |
| 4. リスク分析(災害) | 自然災害 | 2- 4- 1- 13 | Q 自然災害が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 地震・津波・噴火 | 2- 4- 1- 13- 1 | Q 地震・津波・噴火が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 台風・高潮 | 2- 4- 1- 13- 2 | Q 台風・高潮が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 水災・洪水 | 2- 4- 1- 13- 3 | Q 水災・洪水が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 竜巻・風災 | 2- 4- 1- 13- 4 | Q 風害(竜巻・風災)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 落雷 | 2- 4- 1- 13 5 | Q 落雷の経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 雪害 | 2- 4- 1- 13- 6 | Q 雪害の経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 雹害 | 2- 4- 1- 13- 7 | Q 雹害の経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 天候不良・異常気象 | 2- 4- 1- 13- 8 | Q 天候不良・異常気象(長期の日照り、冷夏、暖冬等)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| 5. リスク分析(事故) | 事故 | 2- 4- 1- 14 | Q 事故が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 火災・爆発 | 2- 4- 1- 14- 1 | Q 火災・爆発が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 設備故障 | 2- 4- 1- 14- 2 | Q 設備故障が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 停電 | 2- 4- 1- 14- 3 | Q 停電が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 交通事故 | 2- 4- 1- 14- 4 | Q 交通事故(損害賠償)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 人的損失 | 2- 4- 1- 14- 5 | Q 人的損失(航空機事故・列車事故・船舶事故・交通事故)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 労災事故 | 2- 4- 1- 14- 6 | Q 労災事故(過労死を含む)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 建設中の事故 | 2- 4- 1- 14- 7 | Q 建設中の事故が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 運送中の事故 | 2- 4- 1- 14- 8 | Q 運送中の事故が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 盗難・海賊 | 2- 4- 1- 14- 9 | Q 盗難・海賊が経営に与える影響のリスクを分析していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| リスク分析 | リスク分析 | Ⅱ-4. JRMSのリスク分析 | | | | | |
| 5. リスク分析(事故) | 放射能汚染・放射能漏れ | 2- 4- 1- 14- 10 | Q 放射能汚染・放射能漏れが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 有害微生物、細菌漏洩・バイオハザード | 2- 4- 1- 14- 11 | Q 有害微生物、細菌漏洩・バイオハザードが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 漏水 | 2- 4- 1- 14- 12 | Q 漏水が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 動物害 | 2- 4- 1- 14- 13 | Q 動物の害が経営に与える影響を分析していますか？ | | ● | ● | |
| 6. リスク分析(情報システム) | 情報システム障害 | 2- 4- 1- 15 | Q 情報システム障害が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 停止 | 2- 4- 1- 15- 1 | Q 情報システムの停止(全面、一部停止)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 電子メール使用不可による影響 | 2- 4- 1- 15- 2 | Q 電子メールが使えなくなったときの企業活動に与えるリスクを分析していますか？ | | ● | ● | |
| | 誤作動 | 2- 4- 1- 15- 3 | Q 情報システムの誤作動が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 改ざん | 2- 4- 1- 15- 4 | Q 情報システムの改ざんが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 破壊 | 2- 4- 1- 15- 5 | Q 情報システムの破壊が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 情報漏洩 | 2- 4- 1- 15- 6 | Q 情報システム漏洩が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | セキュリティホール | 2- 4- 1- 15- 7 | Q コンピュータウイルスや不正アクセスに繋がるセキュリティホールへの対策の遅れが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | ネットワーク障害 | 2- 4- 1- 15- 8 | Q コンピュータウイルスや不正アクセスの結果、ネットワーク(インターネット)が大規模な障害になるリスクを分析していますか？ | | ● | ● | |
| 7. リスク分析(経営) | 製品トラブル | 2- 4- 1- 16 | Q 製品トラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 製品瑕疵 | 2- 4- 1- 16- 1 | Q 製品瑕疵が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 製造物責任 | 2- 4- 1- 16- 2 | Q 製造物責任が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | リコール・欠陥製品 | 2- 4- 1- 16- 3 | Q リコール・欠陥製品が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 苦情処理対応トラブル | 2- 4- 1- 16- 4 | Q 苦情処理対応のトラブルリスクを分析していますか？ | | ● | ● | |
| | 知的財産権侵害 | 2- 4- 1- 17 | Q 知的財産権の侵害が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 特許紛争 | 2- 4- 1- 17- 1 | Q 特許紛争が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 実用新案侵害 | 2- 4- 1- 17- 2 | Q 実用新案侵害が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 商標権侵害 | 2- 4- 1- 17- 3 | Q 商標権侵害が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 著作権侵害 | 2- 4- 1- 17- 4 | Q 著作権侵害が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 環境問題 | 2- 4- 1- 18 | Q 環境問題が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 環境規制強化 | 2- 4- 1- 18- 1 | Q 環境規制強化が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 環境賠償責任・環境規則違反 | 2- 4- 1- 18- 2 | Q 環境賠償責任・環境規則違反が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 環境汚染・油濁事故 | 2- 4- 1- 18- 3 | Q 環境汚染・油濁事故が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 廃棄物処理・リサイクル | 2- 4- 1- 18- 4 | Q 廃棄物処理・リサイクルが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 雇用トラブル | 2- 4- 1- 19 | Q 雇用上のトラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 差別 | 2- 4- 1- 19- 1 | Q 差別(国籍、宗教、年齢、性)問題が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 使用者責任 | 2- 4- 1- 19- 2 | Q 使用者責任が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | セクシャルハラスメント | 2- 4- 1- 19- 3 | Q セクシャルハラスメントが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 労働争議・ストライキ・デモ | 2- 4- 1- 19- 4 | Q 労働争議・ストライキ・デモが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 伝染病 | 2- 4- 1- 19- 5 | Q 法定伝染病等が経営に与える影響のリスクを分析していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| リスク分析 | リスク分析 | Ⅱ-4. JRMSのリスク分析 | | | | | |
| 7. リスク分析(経営) | 役員・スタッフの不正、不法行為 | 2- 4- 1- 19- 6 | Q 役員・スタッフの不正、不法行為が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 職場暴力 | 2- 4- 1- 19- 7 | Q 職場暴力が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 集団離職 | 2- 4- 1- 19- 8 | Q 集団離職が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 外国人不法就労 | 2- 4- 1- 19- 9 | Q 外国人不法就労が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 海外従業員の雇用調整 | 2- 4- 1- 19- 10 | Q 海外従業員の雇用調整が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 海外駐在員の安全 | 2- 4- 1- 19- 11 | Q 海外駐在員の安全が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 従業員の高齢化 | 2- 4- 1- 19- 12 | Q 従業員の高齢化が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 法務上のトラブル | 2- 4- 1- 20 | Q 法務上のトラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 商法違反・カルテル | 2- 4- 1- 20- 1 | Q 商法違反・カルテルが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 独禁法違反 | 2- 4- 1- 20- 2 | Q 独禁法違反が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 役員賠償責任 | 2- 4- 1- 20- 3 | Q 役員賠償責任が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | インサイダー取引 | 2- 4- 1- 20- 4 | Q インサイダー取引が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | プライバシー侵害 | 2- 4- 1- 20- 5 | Q プライバシー侵害が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 資産運用トラブル | 2- 4- 1- 21 | Q 資産運用上のトラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | デリバティブ失敗 | 2- 4- 1- 21- 1 | Q 権限の逸脱によるデリバティブの失敗が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 不良債権・貸し倒れ | 2- 4- 1- 21- 2 | Q 不良債権・貸し倒れが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 信用トラブル | 2- 4- 1- 22 | Q 信用トラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 情報管理の不備・顧客情報漏洩 | 2- 4- 1- 22- 1 | Q 情報管理の不備・顧客情報漏洩が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 不正取引・詐欺 | 2- 4- 1- 22- 2 | Q 不正取引・詐欺が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 経営全般トラブル | 2- 4- 1- 23 | Q 経営全般にかかるトラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 企業倫理 | 2- 4- 1- 23- 1 | Q 企業倫理に反する行為が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 取引先倒産 | 2- 4- 1- 23- 2 | Q 取引先(海外を含む)倒産がサプライチェーンに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 格付下落・金融支援の停止 | 2- 4- 1- 23- 3 | Q 格付下落・金融支援の停止が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 経営者の死亡 | 2- 4- 1- 23- 4 | Q 経営者の死亡が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 乱脈経営 | 2- 4- 1- 23- 5 | Q 乱脈経営が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 不適切な宣伝・広告 | 2- 4- 1- 23- 6 | Q 不適切な宣伝・広告が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 不測事態発生時の対応 | 2- 4- 1- 23- 7 | Q 不測事態発生時の広報の不適切さが自社の存続を脅かすリスクを分析していますか？ | | ● | ● | |
| | 社内不正 | 2- 4- 1- 24 | Q 社内不正が経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 共謀犯罪 | 2- 4- 1- 24- 1 | Q 経営者や従業員同士の共謀による(例:本社入金を他支店端末を用いて振替入金し、現金窃取する)犯罪に関するリスクを分析していますか？ | | ● | ● | |
| | 役員のスキャンダル | 2- 4- 1- 24- 2 | Q 役員のスキャンダルが経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 経営者・従業員の不正・犯罪 | 2- 4- 1- 24- 3 | Q 経営資産の管理において経営者や従業員の不正・犯罪に関わるリスクを分析していますか？ | | ● | ● | |
| | 共謀情報漏れ | 2- 4- 1- 24- 4 | Q 経営者や従業員の共謀により不正に重要データを持ち出しあるいは転送した場合の、経営に与える影響のリスクを分析していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるリスクマネジメント計画 | | | | | |
| リスク分析 | リスク分析 | Ⅱ-4. JRMSのリスク分析 | | | | | |
| 8. リスク分析(政治・経済・社会) | 政治的トラブル | 2- 4- 1- 25 | Q 政治的トラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 法律の制定・制度改革・税制改革 | 2- 4- 1- 25- 1 | Q 法律の制定・制度改革・税制改革が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 国際社会の圧力(外圧) | 2- 4- 1- 25- 2 | Q 国際社会の圧力(外圧)が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 貿易制限・通商問題 | 2- 4- 1- 25- 3 | Q 貿易制限・通商問題が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 戦争・内乱 | 2- 4- 1- 25- 4 | Q 戦争・内乱が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 政変・革命 | 2- 4- 1- 25- 5 | Q 政変・革命が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 経済的トラブル | 2- 4- 1- 26 | Q 経済的トラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 経済危機・景気変動 | 2- 4- 1- 26- 1 | Q 経済危機・景気変動が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 株価変動・為替変動・金利変動・地価変動 | 2- 4- 1- 26- 2 | Q 株価変動・為替変動・金利変動・地価変動が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 原料・資材高騰 | 2- 4- 1- 26- 3 | Q 原料・資材高騰が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 社会的トラブル | 2- 4- 1- 27 | Q 社会的トラブルが経営に与える影響のリスクを分析していますか？ | ● | ● | ● | |
| | 市場ニーズの変化 | 2- 4- 1- 27- 1 | Q 市場ニーズの変化が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 社会的影響 | 2- 4- 1- 27- 2 | Q 社会的影響が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 競合・顧客のグローバル化 | 2- 4- 1- 27- 3 | Q 競合・顧客のグローバル化が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 情報技術革新 | 2- 4- 1- 27- 4 | Q 情報技術革新が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | テロ・暴動 | 2- 4- 1- 27- 5 | Q テロ・暴動が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 誘拐・人質 | 2- 4- 1- 27- 6 | Q 誘拐・人質が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 暴力団・総会屋・脅迫 | 2- 4- 1- 27- 7 | Q 暴力団・総会屋・脅迫が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | インターネットによる批判・中傷 | 2- 4- 1- 27- 8 | Q インターネットによる批判・中傷が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | マスコミによる批判・中傷 | 2- 4- 1- 27- 9 | Q マスコミによる批判・中傷が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 風評 | 2- 4- 1- 27- 10 | Q 風評が経営に与える影響のリスクを分析していますか？ | | ● | ● | |
| | 不買運動・消費者運動 | 2- 4- 1- 27- 11 | Q 不買運動・消費者運動が経営に与える影響のリスクを分析していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | RM | ユーザ | |
| リスクマネジメント計画 | リスクマネジメント計画 | Ⅱ. JRMSにおけるマネジメント計画 | | | | | |
| リスク対策 | リスク対策 | Ⅱ-5. JRMSのリスク対策<br>(注)ここではJRMS全般に限定し、情報システム関係については「Ⅳ」で示す。 | | | | | |
| 1. リスク対策の体制 | 事業の継続性 | 2- 5- 1- 1 | Q JRMSのリスク対策では、事業の継続性を考慮していますか？ | ● | ● | ● | |
| | 対策の明確化 | 2- 5- 1- 2 | Q リスク対策の実施についてリスクマネジメント計画上明確にしていますか？ | ● | ● | ● | |
| | 自然災害 | 2- 5- 1- 2- 1 | Q 自然災害に対するリスク対策は明確ですか？ | | ● | ● | |
| | 事故 | 2- 5- 1- 2- 2 | Q 事故に対するリスク対策は明確ですか？ | | ● | ● | |
| | 経営 | 2- 5- 1- 2- 3 | Q 経営に係わるリスク対策は明確ですか？ | | ● | ● | |
| | 政治・経済・社会 | 2- 5- 1- 2- 4 | Q 政治・経済・社会に係わるリスク対策を考慮していますか？ | | ● | ● | |
| | 管理不能リスクの明確化 | 2- 5- 1- 3 | Q リスク対策を実施してもコントロールできないリスクを明確にしていますか？ | ● | ● | ● | |
| | 財務的対応 | 2- 5- 1- 3- 1 | Q リスクコントロールで対処できないリスクへの財務的対応を策定していますか？ | | ● | | |
| | リスク対応のための各種方法組み合わせ | 2- 5- 1- 3- 2 | Q リスク対応のため、リスクファイナンスとリスクコントロールの各種の方法との組合せを実施していますか？ | | ● | | |
| | リスクファイナンス | 2- 5- 1- 4- | Q リスクファイナンス対策は明確ですか？ | ● | ● | | |
| 2. 財務的対応 | 保険リスク | 2- 5- 1- 5- | Q 保険で対処可能なリスクを明確にしていますか？ | | ● | ● | |
| | コンピュータ総合保険 | 2- 5- 1- 5- 1 | Q コンピュータ総合保険に加入していますか？ | | ● | ● | |
| | 利益保険 | 2- 5- 1- 5- 2 | Q 利益保険に加入していますか？ | | ● | ● | |
| | 賠償責任保険 | 2- 5- 1- 5- 3 | Q 賠償責任保険に加入していますか？ | | ● | ● | |
| | コンピュータ機器保険 | 2- 5- 1- 5- 4 | Q コンピュータ機器の保険に加入していますか？ | | ● | | |
| | カントリーリスク | 2- 5- 1- 5- 5 | Q カントリーリスクを明確にしていますか？ | | ● | | |
| | 保有リスク | 2- 5- 1- 5- 6 | Q 保有しているリスクは定められた範囲内としていますか？ | | ● | | |
| | リスクファイナンス見直し | 2- 5- 1- 6 | Q 定期的にリスクファイナンスの見直しを行っていますか？ | | ● | | |
| | 実施関連部署間の協議 | 2- 5- 1- 7 | Q リスクファイナンス実施のため、他の部署の責任者と協議していますか？ | | ● | | |
| 3. リスク対応のための組み合わせ | リスクファイナンス成果評価基準 | 2- 5- 1- 8 | Q リスクファイナンスの成果の評価基準を持っていますか？ | | ● | | |
| 4. テロ | テロ | 2- 5- 1- 9 | Q テロリスクの対策を採用するか否かにつき経営者が決定していますか？ | ● | ● | ● | |
| | テロ対策 | 2- 5- 1- 9- 1 | Q テロリスクについて、リスク分析の結果に基づき対策を講じていますか？ | | ● | ● | |
| | 脅迫・トラブル | 2- 5- 1- 9- 2 | Q 自社への脅迫やトラブル事例を分析して、対策を講じていますか？ | | ● | ● | |
| 5. 人命損失 | 人命損失対策の決定 | 2- 5- 1- 10 | Q 人命損失リスクの対策を採用するか否かにつき経営者および責任者が決定していますか？ | ● | ● | ● | |
| | 人命損失による影響 | 2- 5- 1- 10- 1 | Q 人命損失リスクについて、リスク分析の結果に基づき対策を講じていますか？ | | ● | ● | |
| | 避難訓練 | 2- 5- 1- 10- 2 | Q 経営者、スタッフの避難対策(避難訓練、2方向非常口設置)は実施されていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報セキュリティポリシー | 情報セキュリティポリシー | Ⅲ-1. 情報セキュリティポリシーのリスク分析 | | | | | |
| 1. 情報セキュリティの経営からの視点 | 経営の視点からの分析 | 3- 1- 1- 1 | Q 情報セキュリティポリシーを経営の視点から分析の対象としていますか？ | | ● | | |
| 2. 情報セキュリティポリシーの対象 | リスク分析の対象 | 3- 1- 1- 2 | Q 情報セキュリティポリシーでリスク分析の対象を定めていますか？ | | ● | ● | |
| | 災害 | 3- 1- 1- 2- 1 | Q 災害が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | 障害 | 3- 1- 1- 2- 2 | Q 障害が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | 不正アクセス | 3- 1- 1- 2- 3 | Q 不正アクセスが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | 偽造・不正使用リスク | 3- 1- 1- 2- 4 | Q 情報システムを利用した偽造・不正使用がセキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | コンピュータウイルス | 3- 1- 1- 2- 5 | Q コンピュータウイルスが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | アウトソーシングのリスク | 3- 1- 1- 2- 6 | Q アウトソーシングに関わるリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | SLA | 3- 1- 1- 2- 7 | Q SLAの内容がリスク分析の対象となっていますか？ | | ● | ● | |
| | 緊急時対応 | 3- 1- 1- 3 | Q 緊急時対応の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | ● | |
| | 機密漏洩 | 3- 1- 1- 3- 1 | Q 機密漏洩に対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | 不正アクセス | 3- 1- 1- 3- 2 | Q 不正アクセスに対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | コンピュータウイルス | 3- 1- 1- 3- 3 | Q コンピュータウイルスに対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | ネットワーク障害 | 3- 1- 1- 3- 4 | Q コンピュータウイルスや不正アクセスの結果としてネットワーク（インターネット）が障害になった場合の緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | 災害 | 3- 1- 1- 3- 5 | Q 災害（テロを含む）に対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | 障害 | 3- 1- 1- 3- 6 | Q 障害に対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | 緊急時対応 | 3- 1- 1- 3- 7 | Q バックアップに対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | ファシリティ移動 | 3- 1- 1- 3- 8 | Q その他ファシリティの移動が必要な事態に対する緊急時対応は事前に備えられていますか？ | | ● | ● | |
| | 情報セキュリティ推進組織内容 | 3- 1- 1- 4 | Q 情報セキュリティ推進組織の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | 監査内容 | 3- 1- 1- 4- 1 | Q 監査内容が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| 3. 特筆する情報リスク | 基幹システム情報漏洩（情報） | 3- 1- 1- 5 | Q 基幹情報システムから機密情報が窃取されるリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | ● | |
| | ホームページ（情報） | 3- 1- 1- 6 | Q ホームページに関わる誹謗中傷リスク（被害リスク）が情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | システミックリスク | 3- 1- 1- 7 | Q システミックリスクの影響のリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| | 基幹システムダウン | 3- 1- 1- 8 | Q 基幹システムに関して不正手段による影響のリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？ | | ● | | |
| 4. 時間分析 | 機能停止 | 3- 1- 1- 9 | Q 機能部門別にシステムの機能停止が許される範囲を情報セキュリティポリシーにおいて設定していますか？ | | ● | | |
| 5. 情報リスク洗い出し実施基準 | 情報リスク洗い出し実施基準 | 3- 1- 1- 10 | Q 情報セキュリティポリシーにおいて、情報システムのリスクをもれなく洗い出す基準を定めることを明示してますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－2. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | 3－2－(1) 情報システムのリスク分析 | | | | | |
| 1. IT戦略のリスク分析 | IT戦略のリスク分析 | 3- 2- 1- 1 | Q IT戦略(組織全体の情報システム化戦略)に係わるリスクを分析していますか？ | | ● | ● | |
| | 情報システムの重要度測定 | 3- 2- 1- 1- 1 | Q 情報システムの経営に関する重要度の測定を行っていますか？ | | ● | | |
| | 情報の重要度測定 | 3- 2- 1- 1- 2 | Q 情報(コンテンツ、データ)の経営に関する重要度の測定を行っていますか？ | | ● | | |
| | 業務への影響 | 3- 2- 1- 1- 3 | Q 情報システムが業務に与える影響を分析していますか？ | | ● | ● | |
| | E-Commerce | 3- 2- 1- 1- 4 | Q E-Commerceサービスの提供やサービスの利用の両面からリスクを分析していますか？ | | ● | ● | |
| | 情報リスクと経営存続 | 3- 2- 1- 1- 5 | Q 情報システムに関し、経営の存続を左右すると考えられるリスクを明確に定義していますか？ | | ● | ● | |
| 2. 情報資産リスク | 情報資産リスク | 3- 2- 1- 2 | Q 重要情報資産リスクを分析していますか？ | | ● | ● | |
| | 重要性ランキング | 3- 2- 1- 2- 1 | Q 情報資産の重要性をランキングしていますか？ | | ● | ● | |
| | オーナーの明確化 | 3- 2- 1- 2- 2 | Q 情報資産のオーナーが明確になっていますか？ | | ● | ● | |
| | 機密度ランク | 3- 2- 1- 2- 3 | Q 情報資産の機密度ランクを明確にしていますか？ | | ● | ● | |
| | 可用性維持 | 3- 2- 1- 2- 4 | Q 情報資産の可用性が維持されていますか？ | | ● | ● | |
| | 複数人によるリスク分析 | 3- 2- 1- 2- 5 | Q 情報資産への脅威(リスク)の分析は、関係する組織から視点の異なる複数人の参画を得てなされていますか？ | | ● | ● | |
| | 人的リスク | 3- 2- 1- 3 | Q 重要情報資産に係わる人的リスクを分析していますか？ | | ● | ● | |
| | 改ざんリスク | 3- 2- 1- 3- 1 | Q 情報資産の改ざんのリスクを分析していますか？ | | ● | ● | |
| | 破棄 | 3- 2- 1- 3- 2 | Q 情報システム(ハード、ソフト、メディア)の破棄についてリスクを分析していますか？ | | ● | | |
| | 盗難 | 3- 2- 1- 3- 3 | Q 盗難の情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 物理的侵入 | 3- 2- 1- 3- 4 | Q 物理的な侵入の情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 物理的攻撃 | 3- 2- 1- 3- 5 | Q 物理的な攻撃(爆弾)の情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 倒産 | 3- 2- 1- 3- 6 | Q 情報システム関連のリスクが倒産に結びつくことについてリスクを分析していますか？ | | ● | ● | |
| 3. システム不全 | 機能不全 | 3- 2- 1- 4 | Q 内的、外的理由による機能不全が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | ネットワーク | 3- 2- 1- 4- 1 | Q ネットワークの情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 誤作動 | 3- 2- 1- 4- 2 | Q 誤作動が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 犯罪 | 3- 2- 1- 4- 3 | Q 犯罪が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 対応ミス | 3- 2- 1- 4- 4 | Q 対応ミスによるタイミングの遅れが情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 質低下 | 3- 2- 1- 4- 5 | Q システムの質の低下が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 安全性・機密保持の悪化 | 3- 2- 1- 4- 6 | Q 安全性・機密保持の悪化が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 変化への対応性欠如 | 3- 2- 1- 4- 7 | Q 変化(状況・環境・ニーズ・制度等)への対応性の欠如が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| 4. 適用業務責任・権限 | 適用業務責任・権限 | 3- 2- 1- 5 | Q システムの適用業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | 企画業務 | 3- 2- 1- 5- 1 | Q 企画業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | 開発業務 | 3- 2- 1- 5- 2 | Q 開発業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | 運用業務 | 3- 2- 1- 5- 3 | Q 運用業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | 保守業務 | 3- 2- 1- 5- 4 | Q 保守業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | 予算業務 | 3- 2- 1- 5- 5 | Q 予算業務に関する責任と権限それぞれの機能部門・分野が明確になっていますか？ | | ● | ● | |
| | その他機能分野 | 3- 2- 1- 5- 6 | Q その他の機能分野(　　)に関する責任と権限それぞれの機能部門・分野が明確になっていますか？<br>(該当する機能分野を(　)内に記入して利用) | | ● | ● | |
| 5. 適用業務とリスクマネジメント | 情報システム適用業務 | 3- 2- 1- 6 | Q 情報システム適用業務はリスクマネジメントを前提に構築されていますか？ | | ● | ● | |
| | 設計時の前提 | 3- 2- 1- 7 | Q 適用業務の設計時、リスクマネジメントを前提の1つとしていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－2. 情報システムのリスク分析 | | | | | |
| システム開発 | システム開発 | 3－2－(2)システム開発<br>(システム開発においてアウトソーシングを利用する場合は、「3-2-(4)アウトソーシング」を適用し、評価に用いること):システム開発の各工程で、必要なリスク分析を行っているか？ただし、システム構成等の他の項目でカバーされているものを除く。 | | | | | |
| 1. プロジェクトリスク | プロジェクトリスク | 3- 2- 2- 1 | Q システム開発の対象となる業務について、リスク分析に基づいて、セキュリティの要件が明確になっていますか？ | | ● | ● | |
| | 企画段階 | 3- 2- 2- 2 | Q システム開発に関して企画段階でプロジェクトリスクを分析していますか？ | | ● | ● | |
| | 技術面 | 3- 2- 2- 2- 1 | Q プロジェクト企画段階での技術面(技術的に実現できない)のリスクを分析していますか？ | | ● | ● | |
| | ビジネス面 | 3- 2- 2- 2- 2 | Q プロジェクト企画段階でのビジネス面(システム化の前提条件の変化)のリスクを分析していますか？ | | ● | ● | |
| | 組織面 | 3- 2- 2- 2- 3 | Q プロジェクト企画段階での、組織面(ユーザーが使用しない)のリスクを分析していますか？ | | ● | ● | |
| 2. ライフサイクル | ライフサイクル | 3- 2- 2- 3 | Q 開発ライフサイクルの各工程で、開発のリスクを分析していますか？ | | ● | ● | |
| 3. 開発管理 | 開発管理 | 3- 2- 2- 4 | Q システム開発全般に係わるリスクを分析していますか？ | | ● | ● | |
| | スタッフのスキルの妥当性 | 3- 2- 2- 4- 1 | Q システム開発に関してスタッフのスキルの妥当性のリスクを分析していますか？ | | ● | ● | |
| | コンプライアンス | 3- 2- 2- 4- 2 | Q システム開発に関してコンプライアンスの観点からリスクを分析していますか？ | | ● | ● | |
| | 開発環境 | 3- 2- 2- 4- 3 | Q システム開発に関して開発環境のリスクを分析していますか？ | | ● | ● | |
| | ソフトウェアのサポート切れ | 3- 2- 2- 4- 4 | Q システムソフトウェアのサポート切れのリスクを分析していますか？ | | ● | ● | |
| | ソフトウェアのバージョンアップ | 3- 2- 2- 4- 5 | Q 将来システムソフトウェアのバージョンアップが必要となるリスクを分析していますか？ | | ● | ● | |
| 4. 運用テスト | 運用テスト結果 | 3- 2- 2- 5 | Q 運用テストの結果が、システム要件を満足している度合いについてリスクを分析していますか？ | | ● | ● | |
| | 稼働開始による障害発生 | 3- 2- 2- 5- 1 | Q システム稼働開始のリスクを分析していますか？ | | ● | | |
| | 運用テスト結果 | 3- 2- 2- 5- 2 | Q システム稼働後の処理／応答時間、処理能力のリスクを分析していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－2. 情報システムのリスク分析 | | | | | |
| システム運用 | システム運用 | 3－2－(3) システム運用<br>(システム運用においてアウトソーシングを利用する場合は、「3－2－(4)アウトソーシング」を適用し、評価に用いること) *設備面やシステム構成面でのリスク分析は、他の項目で質問しているので、ここでは運用管理／ミスを対象にリスクを分析する。)* | | | | | |
| 1. システム運用 | 円滑運用 | 3- 2- 3- 1 | Q 円滑なシステム運用を阻害する運用ミスのリスクを考慮した対応策を考えていますか？ | | ● | | |
| 2. 運用管理 | ファイル管理 | 3- 2- 3- 2 | Q ファイル管理についてリスクを考慮した方針を設定していますか？ | | ● | ● | |
| | ライブラリ管理 | 3- 2- 3- 2- 1 | Q ライブラリ管理のリスクを考慮した方針を設定していますか？ | | ● | | |
| | バックアップ | 3- 2- 3- 2- 2 | Q ファイル、データの定期的なバックアップは想定されるリスクを考慮して方針を設定していますか？ | | ● | | |
| | 適用業務管理 | 3- 2- 3- 2- 3 | Q 適用業務管理(例:入出力データの完全性)のリスクを考慮した方針を設定していますか？ | | ● | ● | |
| 3. キャパシティ管理 | キャパシティ管理 | 3- 2- 3- 3 | Q システム資源について不足するリスクの分析を実施していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－2. 情報システムのリスク分析 | | | | | |
| アウトソーシング | アウトソーシング | 3－2－(4)アウトソーシング | | | | | |
| 1. アウトソーサの決定 | アウトソーサの選定手続き | 3- 2- 4- 1 | Q アウトソーサの選定手続きにおいてリスクを分析していますか？ | | ● | | |
| 2. 役割分担 | 契約内容 | 3- 2- 4- 2 | Q アウトソーシングの契約内容についてリスクを分析していますか？ | | ● | ● | |
| | 責任分担 | 3- 2- 4- 2- 1 | Q 委託者と受託者の責任分担のリスクを分析していますか？ | | ● | ● | |
| | 作業内容 | 3- 2- 4- 2- 2 | Q 受託者の作業(業務内容、範囲、スケジュール)内容のリスクを分析していますか？ | | ● | ● | |
| | 変更管理 | 3- 2- 4- 2- 3 | Q アウトソーシング契約での契約内容の変更手続き(作業、契約、システム)のリスクを分析していますか？ | | ● | ● | |
| 3. 守秘義務 | 守秘義務 | 3- 2- 4- 3 | Q 受託者が守秘義務を守らなかった場合のリスクを分析していますか？ | | ● | ● | |
| | 再委託時の守秘義務 | 3- 2- 4- 4 | Q アウトソーシングの再委託を交わす場合の、委託者と同様の守秘義務のリスクを分析していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－3. 情報システムの個別リスク分析 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | 3－3－(1)不正アクセス・コンピュータウイルス関連 | | | | | |
| 1. コンピュータ犯罪のリスク | 経営に与える影響 | 3- 3- 1- 1 | Q コンピュータ犯罪が経営に与える影響(例:サービスの中断や重要な情報流出、企業の不名誉なうわさのひろがり、等)のリスクを分析していますか？ | | ● | ● | |
| | 内部犯罪による信頼への影響 | 3- 3- 1- 1- 1 | Q 内部犯罪の場合、外部の関係者の信頼に与える影響のリスクを分析していますか？ | | ● | | |
| | 経営者・従業員の意識 | 3- 3- 1- 1- 2 | Q 経営者や従業員がコンピュータ犯罪を軽視した場合のリスクを分析していますか？ | | ● | ● | |
| | 盗聴による影響 | 3- 3- 1- 1- 3 | Q 盗聴が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 脅迫による影響 | 3- 3- 1- 1- 4 | Q 脅迫が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 改ざん | 3- 3- 1- 1- 5 | Q 情報システムが改ざんの経営に与える影響のリスクを分析していますか？ | | ● | | |
| | 破壊 | 3- 3- 1- 1- 6 | Q 情報システムの破壊が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 情報漏洩 | 3- 3- 1- 1- 7 | Q 情報システム漏洩が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| 2. 不正アクセスのリスク | モバイル機器盗難 | 3- 3- 1- 2 | Q モバイル機器(パソコン、PDAなど企業外で使う情報機器)の置き忘れ・盗難により重要情報が流出するリスクを分析していますか？ | | ● | ● | |
| | インターネット経由内部犯罪 | 3- 3- 1- 3 | Q 内部者が(社内から)インターネット経由で中継点を変え、再び社内にアクセスすることで情報窃取されるリスクを分析していますか？ | | ● | | |
| | ネッティングリスク | 3- 3- 1- 4 | Q ネッティングに関するリスクを分析していますか？ | | ● | | |
| | 妨害行為 | 3- 3- 1- 5 | Q 悪意によるコンピュータなどへの妨害行為(不正アクセス、改ざん、メール爆弾、DOS)によってサービス中断するリスクを分析していますか？ | | ● | | |
| 3. コンピュータウイルスのリスク | コンピュータウイルス被害・復旧コスト | 3- 3- 1- 6 | Q コンピュータウイルス被害から全面復旧までにかかる費用を分析していますか? | | ● | | |
| | コンピュータウイルス被害による機会損失 | 3- 3- 1- 6- 1 | Q コンピュータウイルス被害によりユーザ業務が受ける機会損失を分析していますか？ | | ● | | |
| | 感染の影響 | 3- 3- 1- 7 | Q コンピュータウイルス感染のリスク(サービス中断など)を分析していますか？ | | ● | ● | |
| | 取引先への影響 | 3- 3- 1- 7- 1 | Q コンピュータウイルス感染により取引先に悪影響や不安を与えるリスクを分析していますか？ | | ● | | |
| | 株価への影響 | 3- 3- 1- 7- 2 | Q コンピュータウイルス感染による株価への影響のリスクを分析していますか？ | | ● | | |
| | 損害賠償請求 | 3- 3- 1- 7- 3 | Q コンピュータウイルス感染により取引先から損害賠償を請求されるリスクを分析していますか？ | | ● | | |
| | ベンダ緊急時対応の遅れ | 3- 3- 1- 8 | Q アンチウイルスに関するベンダのコンピュータウイルスサポート体制をチェックしなかったため、緊急時に対応できない場合のリスクを分析していますか？ | | ● | | |
| | アンチウイルス更新遅れ | 3- 3- 1- 9 | Q アンチウイルスのデータファイルが更新されていなかったため、コンピュータウイルスに対応できず、被害を受けるリスクを分析していますか？ | | ● | | |
| | 定期検診以上の蔓延 | 3- 3- 1- 10 | Q 定期的なウイルスチェックだけでは間に合わず、コンピュータウイルスの蔓延を防ぐことができなかった場合のリスクを分析していますか？ | | ● | ● | |
| 4. 電子メールのリスク | コンピュータウイルス誤配 | 3- 3- 1- 11 | Q 電子メールの利用によってコンピュータウイルスを誤って他社に送ってしまった場合のリスクを分析していますか？ | | ● | ● | |
| 5. ネットワークのリスク | ネットワークの大規模なダウン | 3- 3- 1- 12 | Q コンピュータウイルスや不正アクセスの結果としてネットワーク(インターネット)が大規模障害になり利用できない場合のリスク分析をしていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－3. 情報システムの個別リスク分析 | | | | | |
| 災害別リスク分析 | 災害別リスク分析 | 3－3－(2) 災害 | | | | | |
| 1. 管理 | 情報システムへの影響 | 3- 3- 2- 1 | Q 災害が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 災害復旧手順 | 3- 3- 2- 2 | Q 災害発生時の復旧手順について情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| 2. 災害 | 自然災害 | 3- 3- 2- 3 | Q 自然災害が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 地震・津波・噴火 | 3- 3- 2- 3- 1 | Q 地震・津波・噴火が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 台風・高潮 | 3- 3- 2- 3- 2 | Q 台風・高潮が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 水災・洪水 | 3- 3- 2- 3- 3 | Q 水災・洪水が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 竜巻・風災 | 3- 3- 2- 3- 4 | Q 風害(竜巻・風災)が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 落雷 | 3- 3- 2- 3- 5 | Q 落雷が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 雪害 | 3- 3- 2- 3- 6 | Q 雪害が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 雹害 | 3- 3- 2- 3- 7 | Q 雹害が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 天候不良・異常気象 | 3- 3- 2- 3- 8 | Q 天候不良・異常気象(長期の日照り、冷夏、暖冬等)が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| 3. 事故 | 事故 | 3- 3- 2- 4 | Q 事故が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 火災・爆発 | 3- 3- 2- 4- 1 | Q 火災・爆発が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 停電 | 3- 3- 2- 4- 2 | Q 停電が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 人的損失 | 3- 3- 2- 4- 3 | Q 人的損失(航空機事故・列車事故・船舶事故・交通事故)が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 漏水 | 3- 3- 2- 4- 4 | Q 漏水が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 動物害 | 3- 3- 2- 4- 5 | Q 動物の害が情報システムに与える影響を分析していますか？ | | ● | ● | |
| 4. 人的災害 | 人的災害 | 3- 3- 2- 5 | Q 人的災害が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 戦争・動乱・暴動による影響 | 3- 3- 2- 5- 1 | Q 戦争・動乱・暴動が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 人的リスクの可能性 | 3- 3- 2- 5- 2 | Q 自然災害に乗じて起こる人的リスクの可能性を分析していますか？ | | ● | ● | |
| 5. 委託先リスクの可能性 | 委託先リスクの可能性 | 3- 3- 2- 6 | Q 委託先が災害等の上記リスクを受けた場合のリスクを分析していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク分析 | リスク分析 | Ⅲ. 情報システムのリスク分析 | | | | | |
| 情報システムのリスク分析 | 情報システムのリスク分析 | Ⅲ－3. 情報システムの個別リスク分析 | | | | | |
| 障害 | 障害 | 3－3－(3) 障害 | | | | | |
| 1. 管理 | 情報システムへの影響 | 3- 3- 3- 1 | Q 障害発生時における情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| | 復旧手順 | 3- 3- 3- 2 | Q 障害発生時の復旧手順が情報システムに与える影響のリスクを分析していますか？ | | ● | ● | |
| 2. ハードウェア障害 | ハードウェア障害 | 3- 3- 3- 3 | Q ハードウェア障害(LAN、ファイアウォール等を含む)のリスクを分析していますか？ | | ● | | |
| | ネットワーク(WAN)障害 | 3- 3- 3- 3- 1 | Q ネットワーク(WAN)障害のリスクを分析していますか？ | | ● | | |
| | サーバ障害 | 3- 3- 3- 3- 2 | Q サーバ障害のリスクを分析していますか？ | | ● | | |
| | ISPサービス機能障害 | 3- 3- 3- 3- 3 | Q インターネットサービスプロバイダのサービス機能障害のリスクを分析していますか？ | | ● | | |
| | 端末機器障害 | 3- 3- 3- 3- 4 | Q ユーザまたは端末、クライアント機の障害のリスクを分析していますか？ | | ● | | |
| | 停電 | 3- 3- 3- 3- 5 | Q 停電(UPS障害等)が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| 3. ソフトウェア障害 | ソフトウェア障害 | 3- 3- 3- 4 | Q ソフトウェア障害のリスクを分析していますか？ | | ● | ● | |
| | OS、ライセンスプログラム障害 | 3- 3- 3- 4- 1 | Q サーバのOS、ライセンスプログラムの障害のリスクを分析していますか？ | | ● | | |
| | アプリケーションプログラム停止 | 3- 3- 3- 4- 2 | Q サーバのアプリケーションプログラムが停止した場合のリスクを分析していますか？ | | ● | | |
| | アプリケーションプログラム誤処理 | 3- 3- 3- 4- 3 | Q アプリケーションプログラムの誤処理が情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 端末機器障害 | 3- 3- 3- 4- 4 | Q ユーザまたは端末、クライアント機の障害のリスクを分析していますか？ | | ● | | |
| | その他ソフトウェア障害 | 3- 3- 3- 4- 5 | Q その他ソフトウェアの障害のリスクを分析していますか？ | | ● | | |
| 4. 運用ミス障害 | 運用ミス障害 | 3- 3- 3- 5 | Q 運用ミス障害のリスクを分析していますか？ | | ● | ● | |
| | バックアップ不備 | 3- 3- 3- 5- 1 | Q バックアップの不備によるリスクを分析していますか？ | | ● | | |
| | ソフトウェア更新手続きミス | 3- 3- 3- 6 | Q ソフトウェア更新手続きミスが情報システムに与える影響のリスクを分析していますか？ | | ● | | |
| | 人的リスクの可能性 | 3- 3- 3- 7 | Q オペレーションミスによる消去、誤記入に乗じて起こる人的リスクの可能性を分析していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報セキュリティ | 情報セキュリティ | Ⅳ－1. リスク対策における情報セキュリティ | | | | | |
| 1. 情報セキュリティポリシー | 情報セキュリティポリシー | 4- 1- 1- 1 | Q リスクマネジメントポリシーに基づいて情報セキュリティポリシーを定めていますか？ | | ● | ● | |
| 2. 情報セキュリティポリシーに基づく実施基準 | 情報セキュリティポリシーに基づく実施基準 | 4- 1- 1- 2 | Q 情報セキュリティポリシーに基づく実施基準を定めていますか？ | | ● | ● | |
| | 情報システム総合企画 | 4- 1- 1- 2- 1 | Q 実施基準に情報システム総合企画のリスク対策を定めていますか？ | | ● | ● | |
| | システム開発 | 4- 1- 1- 2- 2 | Q 実施基準にシステム開発のリスク対策を定めていますか？ | | ● | ● | |
| | システム運用 | 4- 1- 1- 2- 3 | Q 実施基準にシステム運用のリスク対策を定めていますか？ | | ● | ● | |
| | アウトソーシング | 4- 1- 1- 2- 4 | Q 実施基準にアウトソーシング関連のリスク対策を定めていますか？ | | ● | ● | |
| | システム監査 | 4- 1- 1- 2- 5 | Q 実施基準にシステム監査を定めていますか？ | | ● | ● | |
| | コンピュータ犯罪 | 4- 1- 1- 2- 6 | Q 実施基準にコンピュータ犯罪対策を定めていますか？ | | ● | ● | |
| | 不正アクセス | 4- 1- 1- 2- 7 | Q 実施基準に不正アクセス対策を定めていますか？ | | ● | ● | |
| | コンピュータウイルス | 4- 1- 1- 2- 8 | Q 実施基準にコンピュータウイルス対策を定めていますか？ | | ● | ● | |
| | E－Commerce | 4- 1- 1- 2- 9 | Q 実施基準にE－Commerce対策を定めていますか？ | | ● | ● | |
| | 電子メール | 4- 1- 1- 2- 10 | Q 実施基準に電子メール利用対策を定めていますか？ | | ● | ● | |
| | 災害対策 | 4- 1- 1- 2- 11 | Q 実施基準に災害対策を定めていますか？ | | ● | ● | |
| | 障害対策 | 4- 1- 1- 2- 12 | Q 実施基準に障害対策を定めていますか？ | | ● | ● | |
| | その他関連項目 | 4- 1- 1- 2- 13 | Q 実施基準にその他関連項目（経営リスク、政治・経済・社会リスク等）を定めていますか？ | | ● | ● | |
| | バックアップ | 4- 1- 1- 2- 14 | Q 実施基準にバックアップ対策を定めていますか？ | | ● | ● | |
| | 緊急時対策 | 4- 1- 1- 2- 15 | Q 実施基準に緊急時対策を定めていますか？ | | ● | ● | |
| | リスクマネジメントシステム計画との整合性 | 4- 1- 1- 3 | Q 実施基準はリスクマネジメントシステム計画と整合性をとって定めていますか？ | | ● | ● | |
| | 企業特性 | 4- 1- 1- 3- 1 | Q 実施基準は企業の特性を重視して作成していますか？ | | ● | ● | |
| | 論理的な構築 | 4- 1- 1- 3- 2 | Q 実施基準の中のリスク対策は情報処理プロセスに沿って論理的に構築されていますか？ | | ● | ● | |
| | 評価リスト | 4- 1- 1- 3- 3 | Q 実施基準は実践的な項目配列、継続的な日常点検、点検結果の評価リストを定めていますか？ | | ● | ● | |
| | 緊急事態復旧計画 | 4- 1- 1- 3- 4 | Q 実施基準は緊急事態発生後の復旧サービスレベル等について定めていますか？ | | ● | ● | |
| | ISO15408との整合性 | 4- 1- 1- 3- 5 | Q 実施基準の策定に関してISO15408（JIS X 5070）との国際的な整合性を考慮していますか？ | | ● | | |
| | ISO17799との整合性 | 4- 1- 1- 3- 6 | Q 実施基準の策定に関してISO17799（JIS X 5080、ISMS）等との国際的な整合性を考慮していますか？ | | ● | | |
| | 実施基準での禁止事項 | 4- 1- 1- 4 | Q 実施基準は禁止事項を定めていますか？ | | ● | ● | |
| | 市販ソフトのコピー使用 | 4- 1- 1- 4- 1 | Q 市販のソフトをコピーして使う行為を禁止していますか？ | | ● | ● | |
| | データ・プログラムの無断使用 | 4- 1- 1- 4- 2 | Q 所有者のあるデータ、プログラムを無断で使う行為を禁止していますか？ | | ● | ● | |
| | 機密情報搾取行為 | 4- 1- 1- 4- 3 | Q イントラネットあるいはLAN情報処理環境に侵入し、機密情報を窃取する行為を禁止していますか？ | | ● | ● | |
| | 覗き見 | 4- 1- 1- 4- 4 | Q 所有者のあるデータ、プログラムを覗き見る行為を禁止していますか？ | | ● | ● | |
| | コンピュータ私用利用 | 4- 1- 1- 4- 5 | Q 会社のコンピュータを私用に使う行為を禁止していますか？ | | ● | ● | |
| | コンピュータウイルス伝染行為 | 4- 1- 1- 4- 6 | Q コンピュータウイルスを伝染させる行為を禁止していますか？ | | ● | ● | |
| | 不正侵入行為 | 4- 1- 1- 4- 7 | Q 他社のシステムへ不正侵入する行為を禁止していますか？ | | ● | ● | |
| | WWWの私用利用 | 4- 1- 1- 4- 8 | Q WWWを仕事以外（個人目的での発注、アンケート回答等）で利用する行為を禁止していますか？ | | ● | ● | |
| | データ不正入力 | 4- 1- 1- 4- 9 | Q 外部端末からインターネットを通じてデータの不正入力を行い、情報撹乱する行為を禁止していますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報セキュリティ | 情報セキュリティ | Ⅳ－1. リスク対策における情報セキュリティ | | | | | |
| 2. 情報セキュリティポリシーに基づく実施基準 | 私用電子メール使用 | 4- 1- 1- 4- 10 | Q 私用の電子メールを受発信する行為を禁止していますか？ | | ● | ● | |
| | ファイルの覗き見行為 | 4- 1- 1- 4- 11 | Q ネットワークにログインしている他者のファイルを許可なく見る行為を禁止していますか？ | | ● | ● | |
| | 仕事以外のファイルの覗き見行為 | 4- 1- 1- 4- 12 | Q 共有サーバにある仕事に関係していないファイルを見る行為を禁止していますか？ | | ● | ● | |
| | 他人のID無断使用 | 4- 1- 1- 4- 13 | Q 他人のIDを無断借用する行為を禁止していますか？ | | ● | ● | |
| | 接続されたマシンの無断操作 | 4- 1- 1- 4- 14 | Q メール、ブラウザ等接続されたままの他者の機器を操作する行為 を禁止していますか？ | | ● | ● | |
| | 時間外でのコンピュータ私用利用 | 4- 1- 1- 4- 15 | Q 時間外に会社のコンピュータでゲームを行う行為を禁止していますか？ | | ● | ● | |
| | 顧客情報の売却 | 4- 1- 1- 4- 16 | Q 業務上入手した顧客情報を正当な理由なしに第3者に売却する行為を禁止していますか？ | | ● | ● | |
| | ホームページによる誹謗中傷行為 | 4- 1- 1- 4- 17 | Q 許可なくホームページを書き換えて会社や組織に対する誹謗中傷する行為を禁止していますか？ | | ● | ● | |
| | 電子掲示板による誹謗中傷行為 | 4- 1- 1- 4- 18 | Q 電子掲示板を用いて特定の組織、人間を誹謗中傷したり、名誉を傷つける行為を禁止していますか？ | | ● | ● | |
| | 動作障害行為 | 4- 1- 1- 4- 19 | Q 情報システムの動作障害を引き起こす行為を禁止していますか？ | | ● | ● | |
| | プログラム・データ改ざん | 4- 1- 1- 4- 20 | Q 正当な理由なくプログラム、データを改ざんする行為を禁止していますか？ | | ● | ● | |
| | 無許可情報の開示行為 | 4- 1- 1- 4- 21 | Q 許可なく情報をシステムを通じて開示する行為を禁止していますか？ | | ● | ● | |
| | スパムメール発信行為 | 4- 1- 1- 4- 22 | Q スパムメールを発信する行為を禁止していますか？ | | ● | ● | |
| | 社会秩序を乱す情報提供 | 4- 1- 1- 4- 23 | Q 社会秩序の安全維持に反する情報の提供を禁止していますか？ | | ● | ● | |
| | コンプライアンス | 4- 1- 1- 5 | Q 実施基準はコンプライアンスに関する事項を定めていますか？ | | ● | ● | |
| | 罰則規程 | 4- 1- 1- 6 | Q 実施基準は禁止事項に反した場合の罰則規定を定めていますか？ | | ● | ● | |
| | 情報オーナーの責任 | 4- 1- 1- 7 | Q 実施基準は機密性の高い個別情報の生成、管理、破棄に至るまでの情報のオーナーの責任と役割について定めていますか？ | | ● | ● | |
| | 自己点検システム・監査システム | 4- 1- 1- 8 | Q 実施基準は内部者の情報システム利用の自己点検、監査について定めていますか？ | | ● | ● | |
| | 実施基準の定期的見直し | 4- 1- 1- 9 | Q 実施基準を定期的に見直していますか？ | | ● | ● | |
| | 企業内教育 | 4- 1- 1- 10 | Q 実施基準は情報システムの利用に関する教育要領を定めていますか？ | | ● | ● | |
| | 情報セキュリティポリシーの徹底 | 4- 1- 1- 11 | Q 情報セキュリティポリシーについての教育等を実施していますか？ | | ● | ● | |
| 3. 情報資産インベントリ | 情報資産目録 | 4- 1- 1- 12 | Q 保護対象の情報資産は漏れなくインベントリ(目録)リストに列挙していますか？ | | ● | ● | |
| | 劣化媒体の排除 | 4- 1- 1- 12- 1 | Q 保護対象インベントリ(目録)から劣化した媒体を排除していますか？ | | ● | | |
| | 重要資産の取扱いと重要装置の仕様 | 4- 1- 1- 12- 2 | Q 実施基準は重要資産および重要装置の仕様の取扱いを定めていますか？ | | ● | | |
| | 機密度ランク | 4- 1- 1- 13 | Q 実施基準は情報の機密度のランクを定めていますか？ | | ● | ● | |
| 4. スタッフ | 情報セキュリティ管理・担当者 | 4- 1- 1- 14 | Q 情報セキュリティ管理者または担当者がいますか？ | | ● | ● | |
| | スタッフ | 4- 1- 1- 14- 1 | Q スタッフに対して強制休暇をとらせる制度がありますか？ | | ● | ● | |
| | 業務ローテーション | 4- 1- 1- 14- 2 | Q スタッフに対してリスクの視点から定期的な業務のローテーションを組んでいますか？ | | ● | ● | |
| | 外部のコンサルタント | 4- 1- 1- 14- 3 | Q 外部のコンサルタントやサービスを利用し、現時点の最善のレベルを追求していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報セキュリティ | 情報セキュリティ | Ⅳ－1. リスク対策における情報セキュリティ | | | | | |
| 5. 情報セキュリティ個別対策 | 操作と業務処理手順 | 4- 1- 1- 15 | Q 実施基準は情報システムに関して操作および業務処理方法等を具体的に示していますか？ | | ● | ● | |
| | 出張、移動中の実施基準 | 4- 1- 1- 16 | Q 実施基準は出張中、移動中の情報セキュリティについて定めていますか？ | | ● | ● | |
| | 携帯端末利用 | 4- 1- 1- 17 | Q 携帯端末を利用している場合、実施基準は携帯端末の利用について定めていますか？ | | ● | ● | |
| | ユーザ認証、アクセス管理 | 4- 1- 1- 17- 1 | Q 実施基準は携帯端末からのユーザ認証、アクセス管理を定めていますか？ | | ● | ● | |
| | 携帯端末紛失連絡体制 | 4- 1- 1- 17- 2 | Q 実施基準は携帯端末を紛失した場合の連絡体制、アクセス禁止等の手続きを定めていますか？ | | ● | | |
| | 情報システム利用手続き | 4- 1- 1- 18 | Q 実施基準は情報システム利用の手続きを定めていますか？ | | ● | ● | |
| | リスク管理文書化 | 4- 1- 1- 19 | Q 実施基準はリスク管理に関する文書化について定めていますか？ | | ● | ● | |
| | データ、媒体利用 | 4- 1- 1- 20 | Q 実施基準はデータや媒体の使用・保管の管理を定めていますか？ | | ● | ● | |
| | ログ確認 | 4- 1- 1- 21 | Q 実施基準は情報のオーナーおよびシステム管理者がアクセスログを定期的に確認するよう定めていますか？ | | ● | | |
| | アクセスログ権限 | 4- 1- 1- 21- 1 | Q 実施基準はアクセスログについてアクセスの権限、権限外の記録方法を定めていますか？ | | ● | | |
| | 機密情報ログ | 4- 1- 1- 21- 2 | Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？ | | ● | | |
| | プログラムソースライブラリ管理 | 4- 1- 1- 22 | Q 実施基準はプログラムソースライブラリの管理・修正・変更の記録についての方法を定めていますか？ | | ● | | |
| | 基幹システムの国際利用 | 4- 1- 1- 23 | Q 基幹システムを国際的に利用している場合、日本との差を把握して情報システムのセキュリティ対策を講じていますか？ | | ● | | |
| | 個人情報保護 | 4- 1- 1- 24 | Q 実施基準は個人情報保護に関して定めていますか？ | | ● | ● | |
| | プロバイダ選定基準 | 4- 1- 1- 25 | Q 実施基準はプロバイダの選定基準を定めていますか？ | | ● | | |
| 6. 自社ホームページ承認 | 自社ホームページ承認 | 4- 1- 1- 26 | Q 実施基準は自社のホームページへの掲載許可について定めていますか？ | | ● | ● | |
| | 掲載許可 | 4- 1- 1- 26- 1 | Q 自社のホームページへの掲載許可についてチェックしていますか？ | | ● | ● | |
| | コンテンツの知的財産権 | 4- 1- 1- 26- 2 | Q 実施基準はコンテンツの知的財産権の審査・登録の制度を定めていますか？ | | ● | ● | |
| | ホームページ記載内容のチェック | 4- 1- 1- 26- 3 | Q HP記載内容の正確性、表現(差別用語等)等をチェックする部署を定めていますか？ | | ● | ● | |
| | コンテンツ侵害への手続き | 4- 1- 1- 27 | Q 実施基準はコンテンツへの侵害があった場合の手続きを定めていますか？ | | ● | ● | |
| | 営業機密漏洩チェック | 4- 1- 1- 27- 1 | Q コンテンツに関して、組織体の営業機密が不用意に漏洩されていないかチェックしていますか？ | | ● | | |
| 7. 教育内容 | 情報システム部門の教育内容 | 4- 1- 1- 28 | Q 情報システム部門の教育訓練の内容に情報システムリスクを網羅していますか？ | | ● | | |
| | 緊急事態対応 | 4- 1- 1- 28- 1 | Q 情報システム部門の教育訓練の内容に緊急事態対応を含んでいますか？ | | ● | | |
| | 誤作動対応 | 4- 1- 1- 28- 2 | Q 情報システム部門の教育訓練の内容に誤作動対応を含んでいますか？ | | ● | | |
| | システム停止対応 | 4- 1- 1- 28- 3 | Q 情報システム部門の教育訓練の内容にシステムの停止対応を含んでいますか？ | | ● | | |
| | システム侵入対応 | 4- 1- 1- 28- 4 | Q 情報システム部門の教育訓練の内容にシステムへの侵入対応を含んでいますか？ | | ● | | |
| | ユーザ部門の教育内容 | 4- 1- 1- 29 | Q ユーザ部門の教育訓練に情報システムリスクを網羅していますか？ | | | ● | |
| | 緊急事態対応 | 4- 1- 1- 29- 1 | Q ユーザ部門の教育訓練に緊急事態対応を含んでいますか？ | | | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報システムのリスク対策 | 情報システムのリスク対策 | Ⅳ－2. 情報システムのリスク対策 | | | | | |
| 情報システム総合企画 | 情報システム総合企画 | 4－2－(1) 情報システム総合企画 | | | | | |
| 1. 実施基準 | 情報システム総合企画 | 4- 2- 1- 1 | Q 実施基準に情報システム総合企画のリスク対策を定めていますか？ | | ● | ● | |
| 2. IT戦略 | 経営戦略との整合 | 4- 2- 1- 2 | Q 経営戦略とIT戦略の整合性(例:経営戦略での業務改革と、それを実現するシステム)がとられていますか？ | | ● | | |
| | 標準ステップ | 4- 2- 1- 3 | Q IT戦略を作成するための標準化されたステップが存在しますか？ | | ● | | |
| | 外部規制 | 4- 2- 1- 4 | Q 実施基準に法、ガイダンス、規程等の外部規制への対応が含まれていますか？ | | ● | | |
| 3. IT計画 | IT戦略とITインフラ計画 | 4- 2- 1- 5 | Q IT戦略とITインフラストラクチャ計画の整合性がとられていますか？ | | ● | | |
| | ITインフラ計画 | 4- 2- 1- 6 | Q ITインフラストラクチャ計画(例:新アプリケーションシステムに必要な技術)が文書としてまとめられていますか？ | | ● | | |
| | 導入計画 | 4- 2- 1- 7 | Q ITインフラストラクチャ計画に基づいて、導入計画が作成されていますか？ | | ● | | |
| 4. 組織体制・機能 | 指揮命令系統 | 4- 2- 1- 8 | Q 情報システム組織として、適切な指揮命令系統が作られていますか？ | | ● | ● | |
| | セキュリティ機能 | 4- 2- 1- 9 | Q 情報システム組織に、適切な情報セキュリティ機能が置かれていますか？ | | ● | ● | |
| | インターナルコントロール機能 | 4- 2- 1- 9- 1 | Q 情報システム組織に、適切なインターナルコントロール機能が置かれていますか？ | | ● | ● | |
| | 品質管理機能 | 4- 2- 1- 9- 2 | Q 情報システム組織に、適切な品質管理機能が置かれていますか？ | | ● | ● | |
| | 決裁権限 | 4- 2- 1- 10 | Q 決済権限を明確に定めていますか？ | | ● | ● | |
| | リスク別担当部門 | 4- 2- 1- 11 | Q リスクの種類に応じて、担当する部門が明確化されていますか？ | | ● | ● | |
| 5. スタッフ | 人事計画 | 4- 2- 1- 12 | Q IT戦略と整合のとれた人事計画が作成されていますか？ | | ● | ● | |
| | スキル | 4- 2- 1- 13 | Q 将来必要となるスキルが識別され、人事計画や教育訓練計画に反映されていますか？ | | ● | ● | |
| | プロジェクト管理スキル | 4- 2- 1- 14 | Q スタッフのプロジェクト管理スキルは、十分ですか？ | | ● | ● | |
| | 品質管理教育 | 4- 2- 1- 15 | Q 品質管理の教育訓練が、適切に行われていますか？ | | ● | ● | |
| 6. 財務 | 投資収益方針 | 4- 2- 1- 16 | Q 投資収益に対する方針が文書化されていますか？ | | ● | ● | |
| | 投資決定方法 | 4- 2- 1- 17 | Q 投資決定に際して、利益実現の方法を明確にしていますか？ | | ● | ● | |
| | 短期的影響の想定 | 4- 2- 1- 17- 1 | Q 投資決定に際して、短期的な影響を想定していますか？ | | ● | ● | |
| | 長期的影響の想定 | 4- 2- 1- 17- 2 | Q 投資決定に際して、長期的な影響を想定していますか？ | | ● | ● | |
| | 他部門への影響の想定 | 4- 2- 1- 17- 3 | Q 投資決定に際して、他部門への影響を想定していますか？ | | ● | ● | |
| | ビジネス上の採算 | 4- 2- 1- 17- 4 | Q 投資決定に際して、ビジネス上の採算を明確にしていますか？ | | ● | ● | |
| | 予定利益 | 4- 2- 1- 18 | Q 予定利益を実現するための経営的な管理が行われていますか？ | | ● | ● | |
| | IT資産管理目録 | 4- 2- 1- 19 | Q IT資産管理のためのインベントリ(目録)が作られていますか？ | | ● | ● | |
| | 関連費用識別 | 4- 2- 1- 20 | Q IT関連費用が全て識別される仕組みがありますか？ | | ● | ● | |
| 7. 管理(文書化を含む) | 全社データ管理 | 4- 2- 1- 21 | Q 全社的なデータ管理の機能が確立されていますか？ | | ● | ● | |
| | 全社データ標準化 | 4- 2- 1- 22 | Q 全社的なデータの標準化が行われていますか？ | | ● | ● | |
| | 全社データ所有者の識別 | 4- 2- 1- 23 | Q データの所有者が識別されていますか？ | | ● | ● | |
| | 管理工程分割 | 4- 2- 1- 24 | Q プロジェクト計画は、成果をチェックできるまでブレークダウンした工程分割がされていますか？ | | ● | ● | |
| | 工程ごとの品質基準 | 4- 2- 1- 25 | Q 品質管理基準は分割された工程ごとに定めていますか？ | | ● | ● | |
| | ライセンス管理 | 4- 2- 1- 26 | Q ライセンス管理を行っていますか？ | | ● | ● | |
| | プロジェクト管理標準 | 4- 2- 1- 27 | Q プロジェクト管理基準が文書化されていますか？ | | ● | ● | |
| | 方法論 | 4- 2- 1- 27- 1 | Q 社内で基準となるシステム開発方法論が文書化されていますか？ | | ● | ● | |
| 8. モニタリング | 規制監視 | 4- 2- 1- 28 | Q 法、ガイダンス、規程類等の外部規制を遵守しているかを監視する機能が存在しますか？ | | ● | ● | |
| | 是正措置 | 4- 2- 1- 29 | Q 必要な是正措置の実施状況が管理されていますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報システムのリスク対策 | 情報システムのリスク対策 | Ⅳ－2. 情報システムのリスク対策 | | | | | |
| システム開発 | システム開発 | 4－2－(2) システム開発 | | | | | |
| 1. 実施基準 | システム開発 | 4- 2- 2- 1 | Q 実施基準にシステム開発のリスク対策を定めていますか？ | | ● | ● | |
| | 決裁実施基準 | 4- 2- 2- 1- 1 | Q 開発プロジェクトにおける決裁権限者、決裁文書等の決裁実施基準が定められていますか？ | | ● | ● | |
| | 開発に応じた決裁 | 4- 2- 2- 1- 2 | Q 決裁実施基準は、プロジェクトの規模に応じて定めていますか？ | | ● | ● | |
| | システム調達のライフサイクルにおけるセキュリティ | 4- 2- 2- 2 | Q システム調達のライフサイクルにおけるプロセスごとの処理実施基準が定められていますか？ | | ● | ● | |
| | 調達 | 4- 2- 2- 2- 1 | Q 情報システムの調達において、情報セキュリティ要件を満たすための明確な実施基準を設けていますか？ | | ● | ● | |
| | 不正防止・機密保護基準 | 4- 2- 2- 2- 2 | Q 情報システムの開発／変更に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？ | | ● | ● | |
| | 破棄基準 | 4- 2- 2- 2- 3 | Q 情報システムの破棄に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？ | | ● | ● | |
| | 品質管理 | 4- 2- 2- 3 | Q 品質管理に関して標準的な手法を定めていますか？ | | ● | ● | |
| | 要員 | 4- 2- 2- 4 | Q 開発要員の管理の観点から明確な実施基準を設けていますか？ | | ● | | |
| | 職務定義 | 4- 2- 2- 4- 1 | Q 各職務に求められる資質や職能を明確に定義していますか？ | | ● | | |
| | 職務分離 | 4- 2- 2- 4- 2 | Q 開発作業における職務分離－開発者・プログラマ・テストスタッフーを実施していますか？ | | ● | | |
| | 情報セキュリティ保持の役割・責任 | 4- 2- 2- 4- 3 | Q 各職務において情報セキュリティに関する役割や責任を明確にしていますか？ | | ● | | |
| | 機密保持合意 | 4- 2- 2- 4- 4 | Q 開発スタッフとの契約において機密保持に関する条項が盛り込まれていますか？ | | ● | | |
| 2. プロジェクト管理 | システム開発方法論 | 4- 2- 2- 5 | Q システム開発プロジェクトにおいて標準的なシステム開発方法論を定めていますか？ | | ● | | |
| | 作業内容と成果物 | 4- 2- 2- 5- 1 | Q プロジェクト開発の各工程について、その作業内容と成果物を定めていますか？ | | ● | | |
| | 技法／ツール | 4- 2- 2- 5- 2 | Q 各工程の開発作業に関して標準的な技法／ツールを定めていますか？ | | ● | | |
| | 判定基準 | 4- 2- 2- 5- 3 | Q 各工程が完了したかの判定基準を定めていますか？ | | ● | | |
| | 進捗管理手続き | 4- 2- 2- 6 | Q 進捗管理に関して標準的な手続きを定めていますか？ | | ● | | |
| 3. システム要件定義 | セキュリティ基準の遵守 | 4- 2- 2- 7 | Q システム要件定義で、セキュリティに関する実施基準を遵守していますか？ | | ● | ● | |
| | 要件の反映 | 4- 2- 2- 7- 1 | Q 情報セキュリティポリシー／実施基準等で定められた要件を反映させていますか？ | | ● | ● | |
| | SLA合意 | 4- 2- 2- 7- 2 | Q 管理指標に関して、SLAとして関係者の合意が取れていますか？ | | ● | ● | |
| | システム要件の反映 | 4- 2- 2- 7- 3 | Q 個人認証、暗号化等のシステム要件がシステム機能に反映されていますか？ | | ● | ● | |
| | システム構成要素の入手可能性 | 4- 2- 2- 8 | Q 情報システムの開発にあたり、システム構成要素（補修部品、消耗品）の入手可能性に関して検討を行いましたか？ | | ● | | |
| 4. プログラム開発 | 開発環境 | 4- 2- 2- 9 | Q 開発環境の維持、管理を適切に実施していますか？ | | ● | | |
| | 機密保持のクラス分け | 4- 2- 2- 9- 1 | Q システムとデータについて、機密保持のクラス分けがなされていますか？ | | ● | | |
| | プログラムライブラリへのアクセス管理 | 4- 2- 2- 9- 2 | Q プログラムライブラリへのアクセス管理は適切に行われていますか？ | | ● | | |
| | 高機密プログラムの保管 | 4- 2- 2- 9- 3 | Q 機密性の高いプログラムの保管に関して、適切な機密保護の対策を実施していますか？ | | ● | | |
| | 設計文書保管 | 4- 2- 2- 9- 4 | Q 設計文書の保管に関して、適切な機密保護の対策を実施していますか？ | | ● | | |
| | 不正ソフトの混入対策 | 4- 2- 2- 9- 5 | Q ウイルス等不正なソフトウェアの混入への対策を実施していますか？ | | ● | | |
| | コンプライアンス | 4- 2- 2- 10 | Q システム開発にあたって、関連する法規、契約等に係わる要求事項を確認していますか？ | | ● | ● | |
| | 知的財産権放棄・契約の要求事項 | 4- 2- 2- 10- 1 | Q 知的財産権に係わる法規、契約に係わる要求事項を確認していますか？ | | ● | ● | |
| | 個人情報保護 | 4- 2- 2- 10- 2 | Q 個人情報保護に係わる法規、契約等に係わる要求事項を確認していますか？ | | ● | ● | |
| | 暗号輸出入管理 | 4- 2- 2- 10- 3 | Q 暗号等の使用に関して、輸出入管理等関連する法規等に係わる要求事項を確認していますか？ | | ● | | |
| | 各国法規遵守 | 4- 2- 2- 10- 4 | Q 国際的な情報システムを構築する場合、各国の規制（例：ECの個人情報保護規定）に遵守すべく必要な措置を講じていますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報システムのリスク対策 | 情報システムのリスク対策 | Ⅳ－2. 情報システムのリスク対策 | | | | | |
| システム開発 | システム開発 | 4－2－(2) システム開発 | | | | | |
| 5. テストデータ | テストデータ | 4- 2- 2- 11 | Q テストデータの作成、保管は適切に実施していますか？ | | ● | ● | |
| | テストの機密保持規定 | 4- 2- 2- 11- 1 | Q 本番データをテストに使用する場合の、機密保持規定が明確化されていますか？ | | ● | ● | |
| | 保護データの排除 | 4- 2- 2- 11- 2 | Q テストデータには、原則として保護すべきデータを含まないようにしていますか？ | | ● | | |
| | 本番データ使用時の保護対策 | 4- 2- 2- 11- 3 | Q テストデータとして本番データを使用する場合には、適切な保護対策を実施していますか？ | | ● | | |
| | 本番データとの分離 | 4- 2- 2- 11- 4 | Q テストデータは、本番データと分離して保管していますか？ | | ● | | |
| 6. 運用テスト | テスト仕様書の内容 | 4- 2- 2- 12 | Q テスト仕様書はテストの目的に照らして適切ですか？ | | ● | ● | |
| | 運用テストの結果 | 4- 2- 2- 13 | Q 運用テストの結果は十分確認していますか？ | | ● | ● | |
| | 導入の妥当性 | 4- 2- 2- 13- 1 | Q 導入の妥当性は十分確認していますか？ | | ● | | |
| | システム性能 | 4- 2- 2- 13- 2 | Q システムの性能は十分把握していますか？ | | ● | | |
| | 操作性確認 | 4- 2- 2- 13- 3 | Q システム運用上の操作性について確認していますか？ | | ● | | |
| | 異常時バックアップ対応 | 4- 2- 2- 13- 4 | Q システム導入後の異常時のバックアップについて対応は十分ですか？ | | ● | | |
| 7. 変更管理 | 管理責任者 | 4- 2- 2- 14 | Q プログラムライブラリの管理責任者が明確になっていますか？ | | ● | | |
| | バージョンアップ手続き | 4- 2- 2- 15 | Q 本番プログラムへのバージョンアップの実施基準が明確になっていますか？ | | ● | | |
| | 管理方針 | 4- 2- 2- 15- 1 | Q 本番プログラムへのバージョンアップについて、全体的な管理方針が明確になっていますか？ | | ● | | |
| | 非常時の実施基準 | 4- 2- 2- 15- 2 | Q 本番プログラムへのバージョンアップについて、非常時の実施基準が明確になっていますか？ | | ● | | |
| | バックアップ・他所保管の実施基準 | 4- 2- 2- 15- 3 | Q バックアップや他所保管の実施基準が明確になっていますか？ | | ● | | |
| | 区分によるバージョンアップ | 4- 2- 2- 16 | Q システムの機密保持の区分により、特別のバージョンアップ手続きが定められていますか？ | | ● | | |
| | 変更管理 | 4- 2- 2- 17 | Q プログラムライブラリの変更は記録されていますか？ | | ● | | |
| | 識別のための体系 | 4- 2- 2- 18 | Q プログラムの重要度を識別するための体系を確立していますか？ | | ● | | |
| | ネーミングルール | 4- 2- 2- 18- 1 | Q プログラムのネーミングルールを確立していますか？ | | ● | | |
| | 高機密プログラム保管 | 4- 2- 2- 19 | Q 機密性の高いプログラムの変更内容は、管理責任者により事前に承認を受けた上で実施されていますか？ | | ● | | |
| | レビュー検証 | 4- 2- 2- 19- 1 | Q 機密性の高いプログラムの変更は、本番前および本番後で独立したレビューにより検証されていますか？ | | ● | | |
| | レビュー内容の文書化 | 4- 2- 2- 19- 2 | Q 機密性の高いプログラム変更について、本番前および本番後のレビュー内容を文書化していますか？ | | ● | | |
| | 管理責任者の承認 | 4- 2- 2- 19- 3 | Q 機密性の高いプログラム変更は管理責任者により承認されていますか？ | | ● | | |
| | 作業とレビューの分離 | 4- 2- 2- 20 | Q 機密性の高いプログラムを開発する場合、開発作業とレビューの職務の分離(例：設計、プログラミング、テスト)が行われていますか？ | | ● | | |
| | アクセスの職務分離 | 4- 2- 2- 21 | Q プログラムの開発／変更を行うプログラマが、本番バージョンのライブラリに対するアクセスが認められないように職務の分離が行われていますか？ | | ● | | |
| | 配布先でのバージョン管理 | 4- 2- 2- 22 | Q クライアントPCにソフトウェアを配布している場合、適切なバージョン管理の手続きが定められていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報システムのリスク対策 | 情報システムのリスク対策 | Ⅳ－2. 情報システムのリスク対策 | | | | | |
| システム運用 | システム運用 | 4－2－(3) システム運用<br>(基本的な流れとして、運用の基準やマニュアルがあり、各レベルの計画が作成され、それに従って運用されているかのチェックと、問題管理が行われることが対策である。) | | | | | |
| 1. 実施基準 | システム運用 | 4- 2- 3- 1 | Q 実施基準にシステム運用のリスク対策を定めていますか？ | | ● | | |
| | システム運用計画 | 4- 2- 3- 1- 1 | Q システム運用計画策定に関する実施基準は、SLAに基づき明確に示されていますか？ | | ● | | |
| 2. システム運用 | システム運用実施 | 4- 2- 3- 2 | Q システムの運用はシステム運用計画どおりに行われていますか？ | | ● | | |
| | 定期的見直し | 4- 2- 3- 2- 1 | Q システム運用計画は定期的に見直されていますか？ | | ● | | |
| | 構成管理 | 4- 2- 3- 3 | Q システム運用上、システム構成管理が適切か、定期的に確認していますか？ | | ● | ● | |
| | 運用マニュアル | 4- 2- 3- 3- 1 | Q 運用マニュアルは常に最新の状態で維持されていますか？ | | ● | ● | |
| | スケジュール運用確認 | 4- 2- 3- 3- 2 | Q 更新された運用マニュアルに従ってシステム運用が行われていることを確認していますか？ | | ● | ● | |
| | 運用手順 | 4- 2- 3- 3- 3 | Q 運用手順は常に適切か、確認していますか？ | | ● | | |
| | データの適切性 | 4- 2- 3- 3- 4 | Q システム運用時の各種データは常に適切か、確認していますか？ | | ● | ● | |
| | スキルの妥当性 | 4- 2- 3- 3- 5 | Q システム運用に関するスタッフのスキルの妥当性について定期的に確認していますか？ | | ● | | |
| 3. モニタリング機能 | 記録・状況把握 | 4- 2- 3- 4 | Q システム運用関連の記録・監視は適切に行われていますか？ | | ● | ● | |
| | 記録・監視 | 4- 2- 3- 4- 1 | Q システムの資源の記録・監視は適切に行われていますか？ | | ● | | |
| | 報告体制 | 4- 2- 3- 4- 2 | Q システム運用の結果(実績)に関する報告(正常終了、異常終了など)の体制は適切ですか？ | | ● | ● | |
| | モニタリング | 4- 2- 3- 5 | Q システム運用に関するモニタリングを実施していますか？ | | ● | | |
| | アプリケーションシステム | 4- 2- 3- 5- 1 | Q アプリケーションシステム自体のモニタリング機能を重視していますか？ | | ● | | |
| | 共用データ | 4- 2- 3- 5- 2 | Q システムで扱う共用データのモニタリングを実施していますか？ | | ● | | |
| | サーバ・クライアント端末 | 4- 2- 3- 5- 3 | Q サーバやクライアント端末のモニタリングを実施していますか？ | | ● | | |
| | ネットワーク | 4- 2- 3- 5- 4 | Q ネットワーク系のモニタリングを実施していますか？ | | ● | | |
| 4. 管理機能 | ファイル世代管理 | 4- 2- 3- 6 | Q ファイルの世代管理は適切に行われているか定期的に確認していますか？ | | ● | ● | |
| | ライブラリ管理 | 4- 2- 3- 6- 1 | Q ライブラリ管理は適切に行われているか定期的に確認していますか？ | | ● | | |
| | 障害管理 | 4- 2- 3- 6- 2 | Q 障害報告書に対して、原因分析、解決策をフォローしていますか？ | | ● | | |
| | 適用業務管理方針 | 4- 2- 3- 6- 3 | Q 適用業務管理(たとえば入出力データの完全性)に対するリスク対策は適切に行われていることを定期的に確認していますか？ | | ● | ● | |
| 5. 復旧時間 | SLA | 4- 2- 3- 7 | Q SLAで示された各アプリケーションシステム障害回復までの時間を考慮した対策を行っていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| アウトソーシング | アウトソーシング | Ⅳ－2－(4)アウトソーシング<br>(ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することを指します。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含みます。) | | | | | |
| 1. 実施基準 | アウトソーシング | 4- 2- 4- 1 | Q 実施基準にアウトソーシング関連のリスク対策を定めていますか？ | | ● | ● | |
| 2. 目的 | TCO | 4- 2- 4- 2 | Q アウトソーシングについて、TCOを認識したマネジメントコントロールが確立されていますか？ | | ● | ● | |
| | コスト削減 | 4- 2- 4- 3 | Q 情報システムに関わるコストの削減がアウトソーシングの目的となっていますか？ | | ● | ● | |
| | スリム化 | 4- 2- 4- 4 | Q システム部門のスリム化がアウトソーシングの目的となっていますか？ | | ● | ● | |
| | 関連技術の安価利用 | 4- 2- 4- 5 | Q 関連技術の安価な利用がアウトソーシングの目的となっていますか？ | | ● | ● | |
| | コスト削減 | 4- 2- 4- 6 | Q コスト削減に通じる技術の専門化、高度化がアウトソーシングの目的となっていますか？ | | ● | ● | |
| 3. 役割分担 | 責任分担 | 4- 2- 4- 7 | Q アウトソーシング契約で、委託者と受託者の責任分担は明確になっていますか？ | | ● | ● | |
| | 役割分担 | 4- 2- 4- 8 | Q アウトソーシング契約で、受託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？ | | ● | ● | |
| | 受託者の作業内容 | 4- 2- 4- 9 | Q 受託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？ | | ● | ● | |
| | 委託者の作業内容 | 4- 2- 4- 10 | Q 委託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？ | | ● | ● | |
| 4. プロジェクト管理 | プロジェクト管理手法 | 4- 2- 4- 11 | Q アウトソーシングした場合のプロジェクト管理手法が明確になっていますか？ | | ● | ● | |
| | 共通開発方法論 | 4- 2- 4- 12 | Q 開発方法論について、両者で共通のものを用いていますか？ | | ● | ● | |
| | 外注委託のレビュー | 4- 2- 4- 13 | Q 委託業務の実施内容をレビューしていますか？ | | ● | ● | |
| | 会議体 | 4- 2- 4- 14 | Q アウトソーシング契約に両者で交わす文書や会議について定められていますか？ | | ● | ● | |
| 5. アウトソーサ管理 | 選定評価基準 | 4- 2- 4- 15 | Q アウトソーサの選定手続きと評価基準が社内で定められていますか？ | | ● | ● | |
| | SLA | 4- 2- 4- 16 | Q アウトソーシング契約に、SLA(サービスレベル合意)を含んでいますか？ | | ● | ● | |
| | ペナルティ | 4- 2- 4- 17 | Q SLAが守れなかった場合のペナルティが定められていますか？ | | ● | ● | |
| | 運用障害時対応 | 4- 2- 4- 18 | Q アウトソーシング契約に、運用障害時の対応(体制、手続き)が定められていますか？ | | ● | ● | |
| | ソフトウェア障害時対応 | 4- 2- 4- 19 | Q ソフトウェア障害時の対応(体制、手続き)が定められていますか？ | | ● | ● | |
| | 品質管理 | 4- 2- 4- 20 | Q 委託作業の品質管理について、体制や手続きが定められていますか？ | | ● | ● | |
| 6. 契約 | 委託契約ルール | 4- 2- 4- 21 | Q 委託契約ルールが定められていますか？ | | ● | ● | |
| | 賠償上限 | 4- 2- 4- 22 | Q アウトソーシング契約で、賠償責任の上限が定められていますか？ | | ● | ● | |
| | 海外委託 | 4- 2- 4- 23 | Q 海外の事業者に委託する場合、各国の輸出入管理規制に遵守すべく必要な措置を講じていますか？ | | ● | ● | |
| | 開発納期延期 | 4- 2- 4- 24 | Q 委託契約で、開発納期が遅延した場合のペナルティが定められていますか？ | | ● | ● | |
| | ソフトウェア瑕疵担保 | 4- 2- 4- 25 | Q ソフトウェア瑕疵担保について定められていますか？ | | ● | ● | |
| | 契約監査 | 4- 2- 4- 26 | Q 委託契約が定められた委託契約ルールに基づいて締結していることを監査していますか？ | | ● | ● | |
| | 受託先監査 | 4- 2- 4- 27 | Q 契約で受託者側に対する監査を行うことが可能となっていますか？ | | ● | ● | |
| | 変更手続き | 4- 2- 4- 28 | Q 契約内容の変更手続き(作業、契約、システム)が定められていますか？ | | ● | ● | |
| 7. 知的財産権 | 再委託 | 4- 2- 4- 29 | Q 再委託を許す場合は、委託者と同様の守秘義務と秘密保持手段が含まれるようになっていますか？ | | ● | ● | |
| | 知的財産権 | 4- 2- 4- 30 | Q 委託契約で、委託先との間で知的財産権を明確にしていますか？ | | ● | ● | |
| | 知的財産権侵害 | 4- 2- 4- 31 | Q 第三者による知的財産権の侵害があった時の責任分担が事前の取り決めによって明確になっていますか？ | | ● | ● | |
| 8. セキュリティ上の留意点 | 委託先情報セキュリティ | 4- 2- 4- 32 | Q 委託契約に、不正防止、機密保護等の対策を盛り込んでいますか？ | | ● | ● | |
| | 委託先情報セキュリティ実施状況 | 4- 2- 4- 33 | Q 委託先における不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じていますか？ | | ● | ● | |
| | 委託先情報セキュリティ遵守 | 4- 2- 4- 34 | Q 発注者の情報セキュリティポリシーと実施基準を遵守することが、要件に含まれていますか？ | | ● | ● | |
| | 秘密保持 | 4- 2- 4- 35 | Q アウトソーシング契約に、受託者の守秘義務と秘密保持手段が含まれていますか？ | | ● | ● | |
| | 再委託時の秘密保持 | 4- 2- 4- 36 | Q アウトソーシング契約で再委託を許す場合は、委託者と同様の守秘義務と秘密保持手段が含まれるようになっていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 情報システムのリスク対策 | 情報システムのリスク対策 | Ⅳ－2. 情報システムのリスク対策 | | | | | |
| システム監査 | システム監査 | 4－2－(5) システム監査(情報セキュリティ監査を含む) | | | | | |
| 1. 実施基準 | システム監査 | 4- 2- 5- 1 | Q 実施基準にシステム監査を定めていますか？ | | ● | ● | |
| 2. 監査 | 重要性の認識 | 4- 2- 5- 2 | Q リスク対応におけるシステム監査の重要性を認識していますか？ | | ● | ● | |
| | システム監査の実施 | 4- 2- 5- 2- 1 | Q システム監査を定期的に実施していますか？ | | ● | ● | |
| | 内部監査 | 4- 2- 5- 2- 2 | Q 内部監査によるシステム監査を実施していますか？ | | ● | ● | |
| | 外部監査 | 4- 2- 5- 2- 3 | Q 外部監査によるシステム監査を実施していますか？ | | ● | ● | |
| | 監査人の選任 | 4- 2- 5- 2- 4 | Q システム監査人を選任していますか？ | | ● | | |
| | リスクマネジメント責任者と監査人の位置づけ | 4- 2- 5- 2- 5 | Q リスクマネジメント責任者とシステム監査人の位置づけは明確ですか？ | | ● | ● | |
| | 報告先 | 4- 2- 5- 3 | Q システム監査の結果は、適切なレベルの経営者に報告されていますか？ | | ● | ● | |
| | 勧告のフォロー | 4- 2- 5- 4 | Q システム監査の勧告をフォローする体制が作られていますか？ | | ● | ● | |
| | 監査未実施 | 4- 2- 5- 5 | Q システム監査を実施していない場合、そのことによるリスクを評価していますか？ | | ● | ● | |
| 3. 監査基準 | 監査基準 | 4- 2- 5- 6 | Q システムに関する全業務(企画、開発、保守、運用)における監査基準は、リスクマネジメントの視点から明確で確実に守られていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| コンピュータ犯罪 | コンピュータ犯罪 | 4－3－(1) コンピュータ犯罪 | | | | | |
| 1. 実施基準 | コンピュータ犯罪 | 4- 3- 1- 1 | Q 実施基準にコンピュータ犯罪(ネットワークを含む)対策を定めていますか？ | | ● | ● | |
| | 内部犯罪対策 | 4- 3- 1- 1- 1 | Q 実施基準に内部犯罪とその対策を定めていますか？ | | ● | | |
| | 個人利用禁止 | 4- 3- 1- 1- 2 | Q 実施基準に情報システムの個人利用の禁止を定めていますか？ | | ● | | |
| | 不正使用対策 | 4- 3- 1- 1- 3 | Q 実施基準に情報システムの不正使用(なりすましなど)対策を定めていますか？ | | ● | | |
| 2. 内部犯罪の防止 | パスワードの変更 | 4- 3- 1- 2 | Q 内部犯罪防止のためにネットワーク利用のパスワードを定期的に変更していますか？ | | ● | | |
| | 内部犯罪の定義 | 4- 3- 1- 2- 1 | Q ネットワーク利用での禁止事項は検出できますか？ | | ● | | |
| | ネットワーク機器 | 4- 3- 1- 3 | Q 内部犯罪防止のため重要なシステム、ネットワークのパスワードを定期的に変更していますか？ | | ● | ● | |
| | 個人使用システム | 4- 3- 1- 4 | Q 個人が日常使用するシステム(パソコンなど)はパスワードを利用していますか？ | | ● | ● | |
| 3. データ保護対策 | データ保護対策 | 4- 3- 1- 5 | Q 重要なデータの保護について、データベースに対策を講じていますか？ | | ● | ● | |
| | 暗号化 | 4- 3- 1- 5- 1 | Q 重要なデータをデータベースに記録する場合、暗号化していますか？ | | ● | ● | |
| | デジタル署名 | 4- 3- 1- 5- 2 | Q 重要なデータをデータベースに記録する場合、(改ざん防止のために)デジタル署名を利用していますか？ | | ● | ● | |
| | 暗合鍵 | 4- 3- 1- 5- 3 | Q 暗号鍵の盗難、搾取、改ざんなどが行われないように管理していますか？ | | ● | ● | |
| | セキュリティホール対策 | 4- 3- 1- 5- 4 | Q コンピュータウイルスに攻撃される可能性のあるセキュリティホールはタイムリーに修正していますか？ | | ● | ● | |
| 4. 盗聴対策 | 盗聴対策 | 4- 3- 1- 6 | Q 盗聴(通信回線の盗聴や室内での特殊機器による盗聴)対策を行っていますか？ | | ● | ● | |
| | 録音機器持込管理 | 4- 3- 1- 6- 1 | Q コンピュータ室への、個人のパソコンや小型デジタル録音装置(録音・記録ができる機器)の持ち込みの管理を行っていますか？ | | ● | ● | |
| | 携帯電話持込 | 4- 3- 1- 6- 2 | Q コンピュータ室への個人の利用の携帯電話機器の持込みを管理していますか？ | | ● | ● | |
| | PDA | 4- 3- 1- 6- 3 | Q 個人が管理するPDAなどに会社関連の重要情報を保存しないようにしていますか(許可する場合は条件を明確に示していますか)？ | | ● | ● | |
| | 無線LAN | 4- 3- 1- 6- 4 | Q 無線LANの利用においては盗聴、データ漏洩対策を行っていますか？ | | ● | | |
| | 電磁波漏れ | 4- 3- 1- 6- 5 | Q ディスプレイの電磁波漏れなどの対策を行っていますか？ | | ● | | |
| 5. 緊急時対応 | ネットワーク対策 | 4- 3- 1- 7 | Q ウイルスの被害でネットワークが使えなくなった場合の緊急時対策(代替通信手段等)を準備していますか？ | | ● | ● | |
| | 外部機関への相談 | 4- 3- 1- 8 | Q コンピュータ犯罪の被害にあたり、関係機関や警察(サイバーポリス)に相談していますか？ | | ● | | |
| | 証拠保全 | 4- 3- 1- 9 | Q コンピュータ犯罪の証拠保全を行っていますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| 不正アクセス | 不正アクセス | 4－3－(2)不正アクセス | | | | | |
| 1. 実施基準 | 不正アクセス | 4- 3- 2- 1 | Q 実施基準に不正アクセス対策を定めていますか？ | | ● | ● | |
| | アクセス権、ID・パスワード付与、チェック体制 | 4- 3- 2- 1- 1 | Q 実施基準にアクセス権、ID・パスワードの付与、チェック体制を定めていますか？ | | ● | | |
| | 物理的アクセス対策 | 4- 3- 2- 1- 2 | Q 実施基準に物理的アクセス対策を定めていますか？ | | ● | | |
| | 論理的アクセス対策 | 4- 3- 2- 1- 3 | Q 実施基準に論理的アクセス対策を定めていますか？ | | ● | | |
| | 外部からのアクセス | 4- 3- 2- 1- 4 | Q 実施基準に外部からのアクセスについて定めていますか？ | | ● | | |
| | 緊急時対策 | 4- 3- 2- 1- 5 | Q 実施基準に不正アクセスが起きた場合の緊急時対策、体制を定めていますか？ | | ● | | |
| 2. アクセス管理 | アクセス管理 | 4- 3- 2- 2 | Q アクセス管理を行っていますか？ | | ● | ● | |
| | 不正アクセス防止 | 4- 3- 2- 2- 1 | Q サーバ、ファイアウォール、ルータなどへの不正アクセス防止策をとっていますか？ | | ● | | |
| | データ保護 | 4- 3- 2- 2- 2 | Q 社外との通信での重要なデータを守る方法(VPNの利用、プロバイダの暗号サービス利用など)をとっていますか？ | | ● | | |
| | 暗号利用 | 4- 3- 2- 2- 3 | Q 重要な通信や重要なファイルについて暗号で保護していますか？ | | ● | | |
| | ID付与 | 4- 3- 2- 3 | Q 職務の必要性に応じて、情報システムへのIDが付与されていますか？ | | ● | ● | |
| | ID・パスワード付与のレビュー | 4- 3- 2- 3- 1 | Q ID、パスワードの付与についてチェックやレビューを行っていますか？ | | ● | | |
| | 不正入手 | 4- 3- 2- 3- 2 | Q ID、パスワードの不正入手があった場合、その不正入手の原因はつきとめられましたか？ | | ● | | |
| | アクセス権付与チェック・レビュー | 4- 3- 2- 3- 3 | Q アクセス権の付与についてチェックやレビューのシステムがありますか？ | | ● | | |
| | 機密度・アクセス制限 | 4- 3- 2- 4 | Q 情報システム上での、機密度のランクと対応したアクセス制限が行われていますか？ | | ● | ● | |
| | 職務分離 | 4- 3- 2- 4- 1 | Q データへのアクセスに対して職務の分離が行われていますか？ | | ● | ● | |
| | インターネット利用 | 4- 3- 2- 5 | Q インターネットの利用について利用条件が定められていますか？ | | ● | ● | |
| | 教育、訓練 | 4- 3- 2- 6 | Q ユーザにアクセス管理の実施方法や基準、概念(need to know)について教育・訓練を実施していますか？ | | ● | ● | |
| | 不正アクセス対策教育 | 4- 3- 2- 6- 1 | Q 情報システム部門のスタッフに対し、不正アクセス対策についての専門的な教育・訓練を実施していますか？ | | ● | | |
| 3. 物理的アクセス対策 | 不正侵入防止 | 4- 3- 2- 7 | Q 入退館システムを通りぬけ、情報システム室、情報ネットワーク管理室に侵入されることを防ぐ仕組みがありますか？ | | ● | ● | |
| | ネットワーク機器の不正防止 | 4- 3- 2- 7- 1 | Q ネットワーク機器などへの物理的アクセス対策(物理的な隔離など)がとられていますか？ | | ● | ● | |
| | 物理的破壊対策 | 4- 3- 2- 7- 2 | Q 所有者以外の者からシステムの物理的破壊を受けることを防げる対策は規定によって義務づけられていますか？ | | ● | ● | |
| 4. 論理的アクセス対策 | 重要なデータ保護対策 | 4- 3- 2- 8 | Q 機密度の高いシステムとデータについて、特別の取扱いが定められていますか？ | | ● | ● | |
| | 暗号 | 4- 3- 2- 8- 1 | Q 通信に暗号を利用していますか？ | | ● | | |
| | デジタル署名 | 4- 3- 2- 8- 2 | Q (改ざん防止のために)デジタル署名を利用していますか？ | | ● | ● | |
| | 暗合鍵管理 | 4- 3- 2- 8- 3 | Q 暗号鍵(公開鍵の秘密鍵や共有鍵)を適切に管理していますか？ | | ● | | |
| | 個人認証 | 4- 3- 2- 9 | Q 個人認証を行っていますか？ | | ● | ● | |
| | 入退室 | 4- 3- 2- 9- 1 | Q 入退室にあたり、パスワード、指紋・虹彩・網膜・顔形状などの確認装置等を設置していますか？ | | ● | ● | |
| | システム個人認証 | 4- 3- 2- 9- 2 | Q 共通に利用するシステムやネットワークでは、ICカード、声紋、指紋等を利用していますか？ | | ● | ● | |
| | 中継地回避の実施基準 | 4- 3- 2- 10 | Q 不正侵入や電子メールの不正中継地とされることを避けるための実施基準は定められていますか？ | | ● | ● | |
| | 中継地懸念とログ分析 | 4- 3- 2- 11 | Q 知らない間にサイバーテロの中継基地とされているのではないかとの疑いをもって、Eメール受信ログ、ホストごとのシステムアプリケーションログの監視を行っていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| 不正アクセス | 不正アクセス | 4－3－(2)不正アクセス | | | | | |
| 5. ネットワーク上のデータ保護 | ネットワークの不正アクセス対策 | 4- 3- 2- 12 | Q ネットワークを介してのアクセスではID、パスワードを利用していますか？ | | ● | ● | |
| | 暗号化転送 | 4- 3- 2- 12- 1 | Q ネットワークを介したアクセスの場合、ID、パスワードは暗号化して転送していますか？ | | ● | | |
| | ファイアウォール | 4- 3- 2- 13 | Q ファイアウォールを設けて(フィルタリングの設定を含む)いますか？ | | ● | | |
| | DMZ | 4- 3- 2- 13- 1 | Q DMZ(バリアセグメント)を儲け、WWW、DNSやメールサーバなどを設置していますか？ | | ● | | |
| | ファイアウォールレイアウト | 4- 3- 2- 13- 2 | Q ファイアウォールが効果的に機能を果たすための機器構成が定められていますか？ | | ● | | |
| | 重要データ保存管理 | 4- 3- 2- 13- 3 | Q 重要なデータを保存管理するサーバはインターネットから直接アクセスできないようにしていますか？ | | ● | | |
| | ログ記録機能 | 4- 3- 2- 13- 4 | Q 重要なデータを管理する情報システムやネットワークシステム(ファイアウォールやアクセスサーバ)にはログを残す機能がありますか？ | | ● | | |
| | ログ自動分析ツール | 4- 3- 2- 13- 5 | Q 当該ログを定期的にチェック(自動で分析するツールの利用も含む)していますか？ | | ● | | |
| | 検知機能 | 4- 3- 2- 13- 6 | Q 不審なアクセスがあった場合、検知(可能であれば追跡)機能を設けていますか？ | | ● | | |
| 6. 外部アクセスからのデータ保護 | 移動体内臓データ保護 | 4- 3- 2- 14 | Q 携帯のパソコンを使っている場合、内蔵しているデータ(会社の重要なデータ)の保護対策を行っていますか？ | | ● | ● | |
| | 接続方式 | 4- 3- 2- 14- 1 | Q 外部からの接続方式については、定期的に対策を見直していますか？ | | ● | ● | |
| | 認証 | 4- 3- 2- 14- 2 | Q 直接ネットワークに接続している場合、呼び返し方式やワンタイムパスワードを利用していますか？ | | ● | ● | |
| | ネットワークサービス | 4- 3- 2- 14- 3 | Q 直接ネットワークに接続している場合、IP-VPN等の安全なネットワークサービスを利用していますか？ | | ● | ● | |
| | ソーシャルエンジニアリング対策 | 4- 3- 2- 14- 4 | Q 電話などでの問い合わせに対してソーシャルエンジニアリング対策を行っていますか？ | | ● | | |
| 7. 不正検出 | アクセスログ確認 | 4- 3- 2- 15 | Q アクセスログについてアクセスの権限、権限外の記録方法について定期的に分析していますか？ | | ● | | |
| | プロトコル | 4- 3- 2- 15- 1 | Q ネットワーク機器は不正アクセスの対象となるプロトコルが検出できる設定になっていますか？ | | ● | | |
| | ログ保存 | 4- 3- 2- 15- 2 | Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？ | | ● | | |
| | ログ確認 | 4- 3- 2- 15- 3 | Q 情報のオーナーおよびシステム管理者が上記ログを定期的に確認していますか？ | | ● | | |
| 8. 緊急時対応 | 緊急対処方法 | 4- 3- 2- 16 | Q ハッカー、ウイルス侵入、不正アクセス等による緊急事態対処のための緊急連絡、対応方法は周知され訓練されていますか？ | | ● | ● | |
| | IPAへの届出 | 4- 3- 2- 17 | Q 不正アクセスの被害にあたりコンピュータ不正アクセス被害届出機関である情報処理振興事業協会(IPA)に被害を届け出ましたか？ | | ● | | |
| | JPCERT/CCへの相談 | 4- 3- 2- 18 | Q 不正アクセスの被害にあたり、JPCERT／CC(JPCERTコーディネーションセンター)に相談していますか？ | | ● | | |
| | 外部機関への相談 | 4- 3- 2- 19 | Q 不正アクセスの被害にあたり、関係機関や警察(サイバーポリス)に相談していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| コンピュータウイルス | コンピュータウイルス | 4－3－(3)コンピュータウイルス | | | | | |
| 1. 実施基準 | コンピュータウイルス対策 | 4- 3- 3- 1 | Q 実施基準にコンピュータウイルス対策(検出・駆除、教育、感染対策)を定めていますか？ | | ● | | |
| | 感染時の緊急時・事後対策 | 4- 3- 3- 1- 1 | Q 実施基準にウイルス感染の場合の緊急時対策、事後対策を定めていますか？ | | ● | | |
| 2. ウイルス検出・駆除 | ウイルス防止ソフト | 4- 3- 3- 2 | Q コンピュータウイルスを防ぐソフトウェアを用意していますか？ | | ● | ● | |
| | ウイルス検出・駆除 | 4- 3- 3- 2- 1 | Q コンピュータウイルスの検出・駆除システム(メールサーバでウイルス検出する場合を含む)がありますか？ | | ● | ● | |
| 3. 教育・訓練 | 教育・訓練 | 4- 3- 3- 3 | Q コンピュータウイルス対策に関して教育・訓練を実施していますか？ | | ● | ● | |
| | システム管理者の教育・訓練 | 4- 3- 3- 3- 1 | Q システム管理者に対し、コンピュータウイルス対策、緊急時対策、感染防止法に関して最新の教育・訓練を実施していますか？ | | ● | ● | |
| | ユーザの教育・訓練 | 4- 3- 3- 4 | Q ユーザにコンピュータウイルス対策に関して定期的に教育・訓練を実施していますか？ | | ● | ● | |
| 4. ウイルス感染対策 | 緊急連絡体制 | 4- 3- 3- 5 | Q コンピュータウイルスに感染した場合の緊急連絡体制ができていますか？ | | ● | ● | |
| | 影響判断 | 4- 3- 3- 5- 1 | Q 仕事への影響をすぐに判断できるようになっていますか？ | | ● | | |
| | 情報収集 | 4- 3- 3- 5- 2 | Q すぐに情報を集め、ウイルスの感染防止や復旧など対処できるようになっていますか？ | | ● | | |
| | 感染ルート | 4- 3- 3- 5- 3 | Q 感染ルートを突き止めることができますか？ | | ● | | |
| | 感染の緊急時対策 | 4- 3- 3- 6 | Q ウイルスに感染した場合に備えた緊急時の対策(システムの再インストール、バックアップデータからの早急な回復など)を有していますか？ | | ● | ● | |
| | ウイルスの感染防止 | 4- 3- 3- 7 | Q 感染したウイルスを送付しないための対策(ソフトでの対策、感染したユーザがパソコンをネットワークから除去するなど)を行っていますか？ | | ● | ● | |
| | 伝染防止対策 | 4- 3- 3- 8 | Q ウイルスの伝染を防ぐための対策がありますか？ | | ● | ● | |
| 5. 事後対策 | 事後対策 | 4- 3- 3- 9 | Q ウイルス感染した場合、事後対策を講じていますか？ | | ● | ● | |
| | 感染情報 | 4- 3- 3- 9- 1 | Q ウイルス感染に関する情報を共有していますか？ | | ● | ● | |
| | 通知 | 4- 3- 3- 9- 2 | Q ウイルス感染の通知を作成し周知していますか？ | | ● | ● | |
| | 対策強化 | 4- 3- 3- 9- 3 | Q ウイルス対策を強化(サーバの導入、ウイルス対策担当者を置くなど)していますか？ | | ● | | |
| | 復旧対策 | 4- 3- 3- 9- 4 | Q ウイルス駆除後のシステムの復旧対策がありますか？ | | ● | | |
| | 再発防止対策 | 4- 3- 3- 9- 5 | Q ウイルス駆除後、再発防止対策がありますか？ | | ● | | |
| | 組織の共有化 | 4- 3- 3- 9- 6 | Q ウイルス感染、駆除の経験は組織で共有化されていますか？ | | ● | ● | |
| | IPAへの届出 | 4- 3- 3- 10 | Q コンピュータウイルス被害届出機関である情報処理振興事業協会(IPA)に被害を届けますか。 | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| E-Commerce | E-Commerce | 4－3－(4)E－Commerce | | | | | |
| 1. 実施基準 | E-Commerce | 4- 3- 4- 1 | Q (E－Commerceサービス提供している場合)実施基準にE－Commerce対策を定めていますか？ | | ● | | |
| | 個人情報保護対策 | 4- 3- 4- 1- 1 | Q 実施基準に個人情報保護対策を定めていますか？ | | ● | | |
| | データ保護対策 | 4- 3- 4- 1- 2 | Q 実施基準にデータ保護対策を定めていますか？ | | ● | | |
| | インターネット利用対策 | 4- 3- 4- 1- 3 | Q 実施基準にインターネット利用に関する対策を定めていますか？ | | ● | | |
| | 電子取引規定 | 4- 3- 4- 1- 4 | Q 実施基準に電子的な取引に関する規定を定めていますか？ | | ● | | |
| 2. プライバシー保護 | プライバシー保護対策 | 4- 3- 4- 2 | Q インターネットでの電子商取引において利用者情報の収集についてはプライバシー保護対策を行っていますか？ | | ● | ● | |
| | コンプライアンスプログラム | 4- 3- 4- 2- 1 | Q 個人情報保護コンプライアンスプログラムを実施していますか？ | | ● | ● | |
| | プライバシーマーク取得 | 4- 3- 4- 2- 2 | Q プライバシーマークの取得(や同等な認証)を受けていますか？ | | ● | ● | |
| | クッキー対策 | 4- 3- 4- 2- 3 | Q クッキーを利用する場合(セッション間で個人を識別するために情報を共有する目的で利用する)の指針を定めていますか？ | | ● | | |
| 3. 不良客情報管理 | 不払い、不良客情報管理 | 4- 3- 4- 3 | Q インターネットでの電子商取引での不払いなどの不良客に対する情報の管理を行っていますか？ | | ● | ● | |
| | 不良客情報入手 | 4- 3- 4- 3- 1 | Q 外部からの不良客などの情報を入手していますか？ | | ● | ● | |
| 4. データ保護対策 | 電子商取引時のデータ保護対策 | 4- 3- 4- 4 | Q インターネットでの電子商取引が増えるにつれて情報が増えていくにあたり、情報が集積されるにつれてデータの保護対策をより強化していますか？ | | ● | ● | |
| | インターネットからの攻撃 | 4- 3- 4- 5 | Q Webサーバに対しインターネットからの攻撃を想定して対策を行っていますか？ | | ● | | |
| | DOS攻撃対策 | 4- 3- 4- 5- 1 | Q DOS攻撃対策を行っていますか？ | | ● | | |
| | アタック対策 | 4- 3- 4- 5- 2 | Q 不正侵入のアタックへの対策を行っていますか？ | | ● | | |
| | セキュリティホール対策 | 4- 3- 4- 5- 3 | Q 迅速なセキュリティホール対策(CERT等の情報に基づき早急なパッチ当てなど)を行っていますか？ | | ● | | |
| | コンピュータウイルス対策 | 4- 3- 4- 5- 4 | Q コンピュータウイルス対策を行っていますか？ | | ● | | |
| | スパムメール対策 | 4- 3- 4- 5- 5 | Q スパムメール対策を行っていますか？ | | ● | | |
| | 改ざん対策 | 4- 3- 4- 5- 6 | Q クロスサイトサブスクリプション対策(信用のできない他サイトへリンクしない)を行っていますか？ | | ● | | |
| 5. ネットワーク機器対応 | ネットワーク機器、サーバの信頼性 | 4- 3- 4- 6 | Q 電子商取引に利用するネットワーク機器、サーバなどの信頼性(二重化や負荷分散)は十分ですか？ | | ● | | |
| | ネットワーク機器、サーバの性能 | 4- 3- 4- 7 | Q 電子商取引に利用するネットワーク機器、サーバなどの性能(能力)は十分ですか？ | | ● | | |
| 6. インターネット接続管理 | インターネット接続の規制 | 4- 3- 4- 8 | Q インターネットの利用について規制していますか？ | | ● | | |
| | インターネット接続機器管理 | 4- 3- 4- 9 | Q インターネットと接続する機器の管理を行っていますか？ | | ● | | |
| | ファイアウォール管理 | 4- 3- 4- 9- 1 | Q ファイアウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？ | | ● | | |
| | IDS | 4- 3- 4- 9- 2 | Q IDS(設置されている場合)の管理を行っていますか？ | | ● | | |
| | DNS管理 | 4- 3- 4- 9- 3 | Q DNS(設置されている場合)の管理を行っていますか？ | | ● | | |
| | 暗号 | 4- 3- 4- 9- 4 | Q ユーザ情報や購入情報などの転送にあたって、暗号を利用し、その暗号鍵の管理、デジタル署名を管理していますか？ | | ● | | |
| | 暗号利用に関する通知 | 4- 3- 4- 9- 5 | Q ユーザに暗号利用に関して通知していますか？ | | ● | | |
| | 不正行為監視 | 4- 3- 4- 9- 6 | Q 利用者への詐欺行為を監視(チェック)していますか？ | | ● | | |
| 7. 電子的証拠 | デジタル署名 | 4- 3- 4- 10 | Q 改ざん防止が必要な場合、デジタル署名や電子認証サービスを利用していますか？ | | ● | | |
| | 時刻証明 | 4- 3- 4- 11 | Q 時刻などの証明が必要な場合、時刻の証明を利用していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 不正アクセス・ウイルス関連 | 不正アクセス・ウイルス関連 | Ⅳ－3. 不正アクセス・コンピュータウイルス関連 | | | | | |
| 電子メール | 電子メール | 4－3－(5)電子メール | | | | | |
| 1. 実施基準 | 電子メール利用対策 | 4- 3- 5- 1 | Q 実施基準に電子メール利用対策を定めていますか？ | | ● | ● | |
| | ユーザ利用 | 4- 3- 5- 1- 1 | Q 実施基準に電子メールのユーザの利用を定めていますか？ | | ● | ● | |
| | サーバ管理 | 4- 3- 5- 1- 2 | Q 実施基準に電子メールサーバの管理を定めていますか？ | | ● | | |
| | インターネット利用 | 4- 3- 5- 1- 3 | Q 実施基準にインターネット利用に関する対策を定めていますか？ | | ● | ● | |
| 2. メールサーバ管理 | メールサーバのデータ保護対策 | 4- 3- 5- 2 | Q メールサーバはデータの改ざんから保護されていますか？ | | ● | | |
| | メールサーバへの攻撃 | 4- 3- 5- 3 | Q メールサーバに対しスパム攻撃を想定して対策を行っていますか？ | | ● | | |
| | DOS攻撃対策 | 4- 3- 5- 3- 1 | Q DOS攻撃対策を行っていますか？ | | ● | | |
| | 不正アクセス対策 | 4- 3- 5- 3- 2 | Q 不正アクセス対策がとられていますか？ | | ● | | |
| | セキュリティホール対策 | 4- 3- 5- 3- 3 | Q セキュリティホール対策を行っていますか？ | | ● | | |
| | コンピュータウイルス対策 | 4- 3- 5- 3- 4 | Q コンピュータウイルス対策を行っていますか？ | | ● | | |
| | 不正メール転送 | 4- 3- 5- 3- 5 | Q 不正を招くおそれのあるメール転送を禁止していますか(例：社外経由で自社メールを転送するなど)？ | | ● | | |
| 3. ネットワーク機器管理 | ネットワーク機器、サーバの信頼性 | 4- 3- 5- 4 | Q 電子メールのネットワーク機器、サーバの信頼性は十分にありますか？ | | ● | | |
| | ネットワーク機器、サーバの性能 | 4- 3- 5- 5 | Q 電子メールのネットワーク機器、サーバなどの性能(能力、記憶容量)は十分にありますか？ | | ● | | |
| | インターネット接続機器管理 | 4- 3- 5- 6 | Q インターネットと接続する機器の管理を行っていますか？ | | ● | | |
| | ファイアウォール管理 | 4- 3- 5- 6- 1 | Q ファイアウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？ | | ● | | |
| | DNS管理 | 4- 3- 5- 6- 2 | Q DNS(設置している場合)の管理を行っていますか？ | | ● | | |
| | 暗号 | 4- 3- 5- 6- 3 | Q 暗号の利用と暗号鍵の管理、デジタル署名の管理を行っていますか？ | | ● | | |
| | 不正行為監視 | 4- 3- 5- 6- 4 | Q 利用者の不正行為を監視(チェック)していますか？ | | ● | | |
| 4. デジタル署名 | デジタル署名 | 4- 3- 5- 7 | Q 改ざん防止が必要な場合、デジタル署名や電子認証サービスを利用していますか？ | | ● | | |
| 5. 悪質メール対策 | 添付ファイル | 4- 3- 5- 8 | Q 添付ファイルによる悪意のあるプログラムを阻止する対策がありますか？ | | ● | | |
| | スクリプト | 4- 3- 5- 9 | Q メールと共に送られてくる不正スクリプトを防止する対策がありますか？ | | ● | | |
| | 不正メール対策 | 4- 3- 5- 10 | Q 送信元のないメールや悪意のあるメールを防止する対策がありますか？ | | ● | | |
| 6. 転送エラー対策 | 転送エラー | 4- 3- 5- 11 | Q 電子メールの不用意な転送エラーによる重要な情報の漏洩対策を行っていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 災害対策 | 災害対策 | Ⅳ－4. 災害対策 | | | | | |
| 1. 実施基準 | 災害対策 | 4- 4- 1- 1 | Q 実施基準に災害対策を定めていますか？ | | ● | ● | |
| | 自然災害対策 | 4- 4- 1- 1- 1 | Q 実施基準に自然災害対策を定めていますか？ | | ● | ● | |
| | 事故災害対策 | 4- 4- 1- 1- 2 | Q 実施基準に事故災害対策を定めていますか？ | | ● | ● | |
| | 人的災害対策 | 4- 4- 1- 1- 3 | Q 実施基準に人的災害対策を定めていますか？ | | ● | ● | |
| 2. 管理 | 経営者の決定 | 4- 4- 1- 2 | Q 災害リスク対策の採用の可否につき経営者により決定されていますか？ | | ● | ● | |
| | 災害復旧レベル | 4- 4- 1- 3 | Q 災害復旧のレベルに関してあらかじめ段階的に決められていますか？ | | ● | ● | |
| | 事業再開 | 4- 4- 1- 3- 1 | Q 事業再開のための最低限のレベルを決めていますか？ | | ● | | |
| | 災害復旧レベル | 4- 4- 1- 3- 2 | Q 災害復旧にあたり、平常時に必要な水準レベルを決めていますか？ | | ● | | |
| | 改善レベル | 4- 4- 1- 3- 3 | Q 復旧にあたり、災害以前以上の改善レベルを決めていますか？ | | ● | | |
| | 是正措置 | 4- 4- 1- 4 | Q 復旧手順について不具合があった場合、是正処置をとっていますか？ | | ● | | |
| | 避難対策 | 4- 4- 1- 5 | Q 経営者、スタッフの避難対策を実施していますか？ | | ● | ● | |
| 3. 防火対策 | 防火壁 | 4- 4- 1- 6 | Q 防火壁を採用していますか？ | | ● | | |
| | コンピュータ室 | 4- 4- 1- 6- 1 | Q コンピュータ室に防火壁を採用していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 6- 2 | Q データ保管場所に防火壁を採用していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 6- 3 | Q ネットワーク設備室に防火壁を採用していますか？ | | ● | | |
| | コンピュータ設置場所 | 4- 4- 1- 6- 4 | Q コンピュータ設置場所に防火壁を採用していますか？ | | ● | | |
| | 自動消火装置 | 4- 4- 1- 7 | Q 自動消火装置を設置していますか？ | | ● | | |
| | コンピュータ室 | 4- 4- 1- 7- 1 | Q コンピュータ室に自動消火装置を設置していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 7- 2 | Q データ保管場所に自動消火装置を設置していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 7- 3 | Q ネットワーク設備室に自動消火装置を設置していますか？ | | ● | | |
| | コンピュータ設置場所 | 4- 4- 1- 7- 4 | Q コンピュータ設置場所に自動消火装置を設置していますか？ | | ● | | |
| | 区画放出対応消火システム | 4- 4- 1- 8 | Q 区画放出対応消火システムを採用していますか？ | | ● | | |
| | コンピュータ室 | 4- 4- 1- 8- 1 | Q コンピュータ室に区画放出対応消火システムを採用していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 8- 2 | Q データ保管場所に区画放出対応消火システムを採用していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 8- 3 | Q ネットワーク設備室に区画放出対応消火システムを採用していますか？ | | ● | | |
| | 消火器 | 4- 4- 1- 9 | Q 消火器を設置していますか？ | | ● | ● | |
| | コンピュータ室 | 4- 4- 1- 9- 1 | Q コンピュータ室に消火器を設置していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 9- 2 | Q データ保管場所に消火器を設置していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 9- 3 | Q ネットワーク設備室に消火器を設置していますか？ | | ● | | |
| | コンピュータ設置場所 | 4- 4- 1- 9- 4 | Q コンピュータ設置場所に消火器を設置していますか？ | | ● | | |
| | 消火栓 | 4- 4- 1- 10 | Q 消火栓を設置していますか？ | | ● | | |
| | コンピュータ室 | 4- 4- 1- 10- 1 | Q コンピュータ室設置フロアに消火栓を設置していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 10- 2 | Q データ保管場所設置フロアに消火栓を設置していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 10- 3 | Q ネットワーク設備室設置フロアに消火栓を設置していますか？ | | ● | | |
| | コンピュータ設置場所 | 4- 4- 1- 10- 4 | Q コンピュータ設置フロアに消火栓を設置していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 災害対策 | 災害対策 | Ⅳ－4. 災害対策 | | | | | |
| 3. 防火対策 | 遮断装置 | 4- 4- 1- 11 | Q 遮断装置を設置していますか？ | | ● | | |
| | コンピュータ室 | 4- 4- 1- 11- 1 | Q コンピュータ室に遮断装置を設置していますか？ | | ● | | |
| | データ保管場所 | 4- 4- 1- 11- 2 | Q データ保管場所に遮断装置を設置していますか？ | | ● | | |
| | ネットワーク設備室 | 4- 4- 1- 11- 3 | Q ネットワーク設備室に遮断装置を設置していますか？ | | ● | | |
| | コンピュータ設置場所 | 4- 4- 1- 11- 4 | Q コンピュータ設置場所に遮断装置を設置していますか？ | | ● | | |
| | 2方向非常口 | 4- 4- 1- 12 | Q 経営者、スタッフの避難対策として2方向非常口を設置していますか？ | | ● | | |
| 4. 耐震対策 | フリーアクセス耐震補強 | 4- 4- 1- 13 | Q コンピュータ室ではフリーアクセスの耐震補強を実施していますか？ | | ● | | |
| | コンピュータ機器の固定 | 4- 4- 1- 14 | Q コンピュータ室では耐震対策としてコンピュータ機器の固定をしていますか？ | | ● | | |
| | 転倒防止 | 4- 4- 1- 15 | Q コンピュータ室では耐震対策としてコンピュータ機器の転倒防止をしていますか？ | | ● | | |
| | 機器・ラックの固定 | 4- 4- 1- 16 | Q データ保管場所では耐震対策として機器およびラックの固定をしていますか？ | | ● | | |
| | テープ落下防止策 | 4- 4- 1- 17 | Q データ保管場所では耐震対策としてテープ等の落下防止策をとっていますか？ | | ● | | |
| | 機器の落下防止策 | 4- 4- 1- 18 | Q コンピュータ設置場所では耐震対策として機器の落下防止策をとっていますか？ | | ● | | |
| | 電源設備 | 4- 4- 1- 19 | Q 電源設備の耐震対策として機器の転倒防止、固定をしていますか？ | | ● | | |
| 5. 水害対策 | コンピュータ室 | 4- 4- 1- 20 | Q コンピュータ室の浸水対策として浸水の恐れのない場所への設置をしていますか？ | | ● | | |
| | 上げ床 | 4- 4- 1- 21 | Q コンピュータ室の浸水対策として上げ床の実施をしていますか？ | | ● | | |
| | 防水堤・ピット | 4- 4- 1- 22 | Q コンピュータ室の浸水対策として防水堤およびピットの設置をしていますか？ | | ● | | |
| | 漏水検知機 | 4- 4- 1- 23 | Q コンピュータ室の浸水対策として漏水検知機の設置をしていますか？ | | ● | | |
| | 排水口 | 4- 4- 1- 24 | Q コンピュータ室の浸水対策として排水口を設置していますか？ | | ● | | |
| | 水落下防止策 | 4- 4- 1- 25 | Q 基幹コンピュータシステムに対する漏水対策として、天井配管から水落下の恐れのない場所への設置をしていますか？ | | ● | | |
| | 吹き込み対策 | 4- 4- 1- 26 | Q 基幹コンピュータシステムに対する漏水対策として、窓からの雨水の吹き込みの恐れのない場所へ機器を設置していますか？ | | ● | | |
| | 防水シート | 4- 4- 1- 27 | Q 基幹コンピュータシステムに対する漏水対策として防水シートの準備をしていますか？ | | ● | | |
| | 電源設備 | 4- 4- 1- 28 | Q 電源設備の水害対策として防水堤の設置をしていますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 障害対策 | 障害対策 | Ⅳ－5. 障害対策 | | | | | |
| 1. 実施基準 | 障害対策 | 4- 5- 1- 1 | Q 実施基準に障害対策を定めていますか？ | | ● | ● | |
| | ハードウェア障害対策 | 4- 5- 1- 1- 1 | Q 実施基準にハードウェア障害対策を定めていますか？ | | ● | ● | |
| | ソフトウェア障害対策 | 4- 5- 1- 1- 2 | Q 実施基準にソフトウェア障害対策を定めていますか？ | | ● | ● | |
| | 運用ミス障害 | 4- 5- 1- 1- 3 | Q 実施基準に運用ミス障害対策を定めていますか？ | | ● | ● | |
| 2. 管理 | 障害対策 | 4- 5- 1- 2 | Q 情報システムの障害対策を実施していますか？ | | ● | | |
| | 運用監視機能 | 4- 5- 1- 2- 1 | Q 運用監視機能を設置していますか？ | | ● | | |
| | 障害検出機能 | 4- 5- 1- 2- 2 | Q 障害検出機能を設置していますか？ | | ● | | |
| | 縮退運転機能 | 4- 5- 1- 2- 3 | Q 縮退運転機能を設置していますか？ | | ● | | |
| | 代替運転機能 | 4- 5- 1- 2- 4 | Q 代替運転機能を設置していますか？ | | ● | | |
| | 回復機能 | 4- 5- 1- 2- 5 | Q 回復機能を設置していますか？ | | ● | | |
| | サービスレベル | 4- 5- 1- 3 | Q 障害対策に関してサービスレベルを取り決めていますか？ | | ● | ● | |
| | ポリシーとの整合性 | 4- 5- 1- 3- 1 | Q SLA(サービスレベル合意)で取り決めた内容は、情報セキュリティポリシーの要件を満たしていますか？ | | ● | ● | |
| | 管理責任者の承認 | 4- 5- 1- 3- 2 | Q SLAで示された内容に関して、アプリケーションの管理責任者の承認を得ていますか？ | | ● | ● | |
| | トランザクション量 | 4- 5- 1- 3- 3 | Q SLAでシステムへ入力するトランザクション量が示されていますか？ | | ● | ● | |
| | トランザクション量の測定 | 4- 5- 1- 3- 4 | Q SLAで示されたシステムへ入力するトランザクション量は、定期的に測定を行い結果を記録していますか？ | | ● | | |
| 3. 手続き | ソフトウェア更新手続き | 4- 5- 1- 4 | Q ソフトウェアの更新手続きについて明確になっていますか？ | | ● | ● | |
| | 最終テスト結果確認 | 4- 5- 1- 4- 1 | Q アプリケーションの管理責任者が最終テスト結果を確認していますか？ | | ● | ● | |
| | 更進記録整備 | 4- 5- 1- 4- 2 | Q すべての更新記録を整備していますか？ | | ● | | |
| | 記録内容 | 4- 5- 1- 4- 3 | Q 更新記録と許可内容を一致させる手順を明確にしていますか？ | | ● | | |
| | 更新確認 | 4- 5- 1- 5 | Q ソフトウェアの更新について、手続きどおりに実施されているか定期的な確認が行われていますか？ | | ● | | |
| | ソフトウェア更新 | 4- 5- 1- 6 | Q ソフトウェアの更新手続きについての各項目は、その妥当性について定期的に評価し、不具合の是正処置をとっていますか？ | | ● | | |
| | 障害管理票 | 4- 5- 1- 7 | Q すべての障害についての障害管理票の作成要領を定めていますか？ | | ● | | |
| | 変更後障害 | 4- 5- 1- 8 | Q プログラム変更後に障害が発生した時に、変更前のプログラムに戻す手続きが文書化されていますか？ | | ● | | |
| 4. 情報システム | ディスク障害対策 | 4- 5- 1- 9 | Q ディスク障害対策として、重要なディスクドライブは冗長な構成がとられていますか？ | | ● | | |
| 5. ユーティリティ | 施設障害対策 | 4- 5- 1- 10 | Q 施設の障害対策を講じていますか？ | | ● | | |
| | 適用業務優先順位 | 4- 5- 1- 10- 1 | Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？ | | ● | | |
| | 無停電装置 | 4- 5- 1- 10- 2 | Q 主要な機器の電源は無停電装置(含む自家発電装置)から供給されていますか？ | | ● | | |
| | 無停電装置テスト | 4- 5- 1- 10- 3 | Q 設置した無停電装置(含む自家発電装置)は定期的にテストが行われていますか？ | | ● | | |
| | 供給能力 | 4- 5- 1- 10- 4 | Q 無停電装置の供給能力は、計画された拡張も含む機器構成に対して十分ですか？ | | ● | | |
| | 空調設備の多重化 | 4- 5- 1- 10 5 | Q 空調設備は、室内設備および屋外設備ともに多重化されていますか？ | | ● | | |
| | 水冷 | 4- 5- 1- 10- 6 | Q 空調設備が水冷の場合、水冷用の予備水を確保していますか？ | | ● | | |
| 6. ネットワーク対策 | 回線障害対策 | 4- 5- 1- 11 | Q 回線障害対策を実施していますか？ | | ● | | |
| | 避雷針 | 4- 5- 1- 11- 1 | Q 交換機に避雷針を設置していますか？ | | ● | | |
| | ネットワーク障害対策 | 4- 5- 1- 11- 2 | Q ネットワーク障害対策を実施していますか？ | | ● | | |
| 7. 復旧 | 復旧レベル | 4- 5- 1- 12 | Q 障害復旧のレベルを定めていますか？ | | ● | ● | |
| | 代替手段 | 4- 5- 1- 12- 1 | Q 必要な場合の代替手段を講じていますか？ | | ● | ● | |
| | 是正措置 | 4- 5- 1- 12- 2 | Q 復旧手順について不具合があった場合、是正処置をとっていますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| その他 | その他 | Ⅳ－6. その他関連項目 | | | | | |
| 1. 実施基準 | その他関連項目 | 4- 6- 1- 1 | Q 実施基準にその他関連項目を定めていますか？ | | ● | ● | |
| | 経営リスク | 4- 6- 1- 1- 1 | Q 実施基準に経営リスクに関する対策を定めていますか？ | | ● | ● | |
| | 政治・経済・社会リスク | 4- 6- 1- 1- 2 | Q 実施基準に政治・経済・社会リスクに関する対策を定めていますか？ | | ● | ● | |
| | テロ対策 | 4- 6- 1- 1- 3 | Q 実施基準にテロに対する対策を定めていますか？ | | ● | ● | |
| 2. サービス提供 | 会員規約 | 4- 6- 1- 2 | Q サービス提供にあたり利用者の会員規約を定めていますか？ | | ● | ● | |
| | 規約違反 | 4- 6- 1- 3 | Q サービス提供の停止となる規約違反事項を明確にし、会員に説明していますか？ | | ● | ● | |
| | 通信の秘密保護教育 | 4- 6- 1- 4 | Q サービス提供の実務に携わっている管理者に対し、「通信の秘密保護（電気通信事業法第4条）」について教育を行っていますか？ | | ● | ● | |
| 3. ユーザ間トラブル | ユーザ間トラブル対策の決定 | 4- 6- 1- 5 | Q ユーザとの間のサービス、契約等に関するトラブルリスクの対策を採用するか否かにつき経営者が決定していますか？ | | ● | ● | |
| | ユーザ間トラブル対策 | 4- 6- 1- 5- 1 | Q ユーザ間トラブルリスクについての分析の結果、対策を講じていますか？ | | ● | ● | |
| | 法的責任・事後対応 | 4- 6- 1- 5- 2 | Q 会員が提供しているサービスを利用して違法行為を行った場合について事前にシナリオを作成し、サービス提供企業（自社）の法的責任および事後対応について検討していますか？ | | ● | ● | |
| | 法的責任・事後対応対象 | 4- 6- 1- 5- 3 | Q 会員間で提供しているサービスの利用の結果トラブルが発生した場合について事前にシナリオを作成し、サービス提供企業（自社）の法的責任および事後対応について対象を定めていますか？ | | ● | ● | |
| 4. 苦情処理対応 | 苦情処理対応の決定 | 4- 6- 1- 6 | Q 苦情処理対応トラブルリスクの対策を採用するか否かにつき経営者および責任者が決定していますか？ | | ● | ● | |
| | 苦情処理対応策 | 4- 6- 1- 6- 1 | Q 苦情処理対応におけるトラブルリスクについて対策を講じていますか？ | | ● | ● | |
| | 苦情処理対応マネジメントシステム | 4- 6- 1- 6- 2 | Q サービス提供に対する苦情処理対応マネジメントシステムを導入していますか？ | | ● | ● | |
| 5. 危機管理計画徹底 | 危機管理計画の内外関係者への徹底 | 4- 6- 1- 7 | Q 危機管理計画は、資産の喪失・破壊に関してユーザ、アウトソーサも含め関係者に周知徹底されていますか？ | | ● | ● | |
| | 物的資産喪失・破壊 | 4- 6- 1- 7- 1 | Q 物的資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ | | ● | ● | |
| | 情報資産喪失・破壊 | 4- 6- 1- 7- 2 | Q 情報資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ | | ● | ● | |
| | その他資産喪失・破壊 | 4- 6- 1- 7- 3 | Q その他の資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？ | | ● | ● | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| バックアップ | バックアップ | Ⅳ－7. バックアップ | | | | | |
| 1. 実施基準 | バックアップ対策 | 4- 7- 1- 1 | Q 実施基準にバックアップ対策を定めていますか？ | | ● | ● | |
| 2. 二重化対策 | 二重化対策 | 4- 7- 1- 2 | Q 情報システムのバックアップ対策(二世代保存を含む)を実施していますか？ | | ● | | |
| | 交換機、チャネル | 4- 7- 1- 2- 1 | Q 交換機、チャネルの二重化を行っていますか？ | | ● | | |
| | 機器 | 4- 7- 1- 2- 2 | Q 機器の二重化を行っていますか？ | | ● | | |
| | LAN | 4- 7- 1- 2- 3 | Q LANの二重化を行っていますか？ | | ● | | |
| | WAN | 4- 7- 1- 2- 4 | Q WANの二重化を行っていますか？ | | ● | | |
| | 切り替えテスト | 4- 7- 1- 3 | Q バックアップ機器への切り替えテストが実施され、その結果の評価が行われていますか？ | | ● | | |
| 3. ファイルのバックアップ | プログラムバックアップ | 4- 7- 1- 4 | Q プログラムのバックアップを行っていますか？ | | ● | | |
| | 実施方法 | 4- 7- 1- 4- 1 | Q プログラムファイルバックアップの実施方法は明確ですか？ | | ● | | |
| | 遠隔地保管 | 4- 7- 1- 4- 2 | Q プログラムファイルバックアップの遠隔地保管を行っていますか？ | | ● | | |
| | 同一サイト内保管 | 4- 7- 1- 4- 3 | Q プログラムファイルバックアップの同一サイト内保管を行っていますか？ | | ● | | |
| | OSファイルバックアップ | 4- 7- 1- 5 | Q OSファイルのバックアップを行っていますか？ | | ● | | |
| | 実施方法 | 4- 7- 1- 5- 1 | Q OSファイルバックアップの実施方法は明確ですか？ | | ● | | |
| | 遠隔地保管 | 4- 7- 1- 5- 2 | Q OSファイルバックアップの遠隔地保管を行っていますか？ | | ● | | |
| | 同一サイト内保管 | 4- 7- 1- 5- 3 | Q OSファイルバックアップの同一サイト内保管を行っていますか？ | | ● | | |
| | データファイルバックアップ | 4- 7- 1- 6 | Q データファイルのバックアップを行っていますか？ | | ● | ● | |
| | 実施方法 | 4- 7- 1- 6- 1 | Q データファイルバックアップの実施方法は明確ですか？ | | ● | | |
| | 遠隔地ミラーデータ | 4- 7- 1- 6- 2 | Q データファイルはリアルタイムで遠隔地ミラーデータを作成していますか？ | | ● | | |
| | 遠隔地保管 | 4- 7- 1- 6- 3 | Q データファイルバックアップの遠隔地保管を行っていますか？ | | ● | | |
| | 同一サイト内保管 | 4- 7- 1- 6- 4 | Q データファイルバックアップの同一サイト内保管を行っていますか？ | | ● | | |
| | 保存期間 | 4- 7- 1- 6- 5 | Q データの保存期間は示されていますか？ | | ● | | |
| | バックアップ頻度 | 4- 7- 1- 6- 6 | Q 機能停止許容時間内に復旧ができる頻度でバックアップを実施していますか？ | | ● | | |
| | DBファイルバックアップ | 4- 7- 1- 7 | Q DBファイルのバックアップを行っていますか？ | | ● | | |
| | 実施方法 | 4- 7- 1- 7- 1 | Q DBファイルバックアップの実施方法は明確ですか(バックアップ頻度、バックアップ取得方法、保管場所)？ | | ● | | |
| | 遠隔地ミラーDB | 4- 7- 1- 7- 2 | Q DBファイルはリアルタイムで遠隔地ミラーDBを作成していますか？ | | ● | | |
| | 遠隔地保管 | 4- 7- 1- 7- 3 | Q DBファイルバックアップの遠隔地保管を行っていますか？ | | ● | | |
| | 同一サイト内保管 | 4- 7- 1- 7- 4 | Q DBファイルバックアップの同一サイト内保存を行っていますか？ | | ● | | |
| | ボリューム | 4- 7- 1- 7- 5 | Q ボリューム単位でバックアップを取得している場合、必要なボリュームはすべて対象となっていますか？ | | ● | | |
| | 災害時用同一ディスク保有 | 4- 7- 1- 7- 6 | Q ボリューム単位でバックアップを取得している場合、災害時用に同一モデルのディスクを確保していますか？ | | ● | | |
| | ログバックアップ | 4- 7- 1- 7- 7 | Q DBMSのログは、定期的にバックアップされていますか？ | | ● | | |
| | ログの分別化 | 4- 7- 1- 7- 8 | Q DBMSのログは、データベース本体と別のディスクを使用していますか？ | | ● | | |
| 4. ネットワーク対策 | 代替回線 | 4- 7- 1- 8 | Q 代替回線を確保していますか？ | | ● | | |
| | 代替機 | 4- 7- 1- 9 | Q 代替機を準備していますか？ | | ● | | |
| | 手作業による代替手段 | 4- 7- 1- 9- 1 | Q 手作業による代替手段を準備していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| バックアップ | バックアップ | Ⅳ－7. バックアップ | | | | | |
| 5. 予備サイト | 予備サイト設置 | 4- 7- 1- 10 | Q 情報システムの予備サイトを設置していますか？ | | ● | | |
| | 同一室内のバックアップ用コンピュータ | 4- 7- 1- 10- 1 | Q 同一コンピュータ室内にバックアップ用のコンピュータを設置していますか？ | | ● | | |
| | 同一建物内のバックアップ用コンピュータ | 4- 7- 1- 10- 2 | Q 同一建物内の別室にバックアップ用のコンピュータを設置していますか？ | | ● | | |
| | バックアップセンタ | 4- 7- 1- 10- 3 | Q 情報喪失に備えて、平時からのバックアップセンタが準備されていますか？ | | ● | | |
| | 遠隔地バックアップセンタ | 4- 7- 1- 10- 4 | Q 遠隔地にバックアップセンタを設置していますか？ | | ● | | |
| | バックアップサービス業者 | 4- 7- 1- 10- 5 | Q バックアップサービス業者と契約していますか？ | | ● | | |
| | 相互バックアップ契約 | 4- 7- 1- 10- 6 | Q 同種コンピュータのユーザと相互バックアップ契約を締結していますか？ | | ● | | |

| キーワード | キーワード | 識別コード | 質問項目 | 回答者 | | | 備考 |
|---|---|---|---|---|---|---|---|
| | | | | 経営者 | IS | ユーザ | |
| リスク対策 | リスク対策 | Ⅳ. 情報システムにおけるリスク対策 | | | | | |
| 緊急時対策 | 緊急時対策 | Ⅳ－8. 緊急時対策 | | | | | |
| 1. 実施基準 | 緊急時対策 | 4- 8- 1- 1 | Q 実施基準に緊急時対策を定めていますか？ | | ● | | |
| | 障害発生 | 4- 8- 1- 1- 1 | Q 実施基準に障発生時の緊急時対策を定めていますか？ | | ● | | |
| | 機密漏洩対策 | 4- 8- 1- 1- 2 | Q 実施基準に機密漏洩に対する緊急時対策を定めていますか？ | | ● | | |
| | 不正アクセス | 4- 8- 1- 1- 3 | Q 実施基準に不正アクセスに対する緊急時対策を定めていますか？ | | ● | | |
| | マクロウイルス | 4- 8- 1- 1- 4 | Q 実施基準にマクロウイルスに対する緊急時対策を定めていますか？ | | ● | | |
| | 自然災害 | 4- 8- 1- 1- 5 | Q 実施基準に自然災害に対する緊急時対策を定めていますか？ | | ● | | |
| | 倒産 | 4- 8- 1- 1- 6 | Q 実施基準にアウトソース先の倒産による緊急時対策を定めていますか？ | | ● | | |
| | 法令侵害 | 4- 8- 1- 1- 7 | Q 実施基準に各種法令侵害に対する緊急時対策を定めていますか？ | | ● | | |
| | バックアップ | 4- 8- 1- 1- 8 | Q 実施基準にバックアップに対する緊急時対策を定めていますか？ | | ● | | |
| | ファシリティ移動 | 4- 8- 1- 1- 9 | Q 実施基準にその他ファシリティの移動が必要な事態に対する緊急時対策を定めていますか？ | | ● | | |
| 2. 事前対応 | 緊急時対応の訓練 | 4- 8- 1- 2 | Q 緊急事態発生時の対応について情報セキュリティの面からスタッフに対して定期的に訓練を行っていますか？ | | ● | | |
| 3. 緊急時対応手続き | 緊急時対応手続きの明確化 | 4- 8- 1- 3 | Q 緊急時対策における手続きは明確ですか？ | | ● | ● | |
| | 緊急連絡網 | 4- 8- 1- 3- 1 | Q 緊急連絡網を整備していますか？ | | ● | ● | |
| | 緊急時対応体制 | 4- 8- 1- 3- 2 | Q 緊急時対応体制を明確にしていますか？ | | ● | ● | |
| | 代替対応手順 | 4- 8- 1- 3- 3 | Q 緊急時の代替対応手順を明確にしていますか？ | | ● | ● | |
| | 障害解決のフローチャート化 | 4- 8- 1- 3- 4 | Q 発生した障害について、解決までの業務をフローチャート化していますか？ | | ● | ● | |
| | 教育訓練計画 | 4- 8- 1- 3- 5 | Q 緊急事態を想定した教育訓練計画を作成していますか？ | | ● | ● | |
| | 対策本部 | 4- 8- 1- 3- 6 | Q 緊急時対策本部の組織と物理的な設定基準はあらかじめ定められていますか？ | | ● | ● | |
| | 判定基準 | 4- 8- 1- 3- 7 | Q 情報資産に関する緊急事態の判定基準は明確ですか？ | | ● | | |
| | 緊急事態宣言 | 4- 8- 1- 3- 8 | Q 緊急事態宣言(シナリオ)と通知方法は事前に決められていますか？ | | ● | ● | |
| | 情報資産 | 4- 8- 1- 3- 9 | Q 情報資産固有の緊急事態対応手順はあらかじめ定められていますか？ | | ● | | |
| | 不審・異常ログ発見時の通報手順 | 4- 8- 1- 3- 10 | Q 不審・異常ログの発見とシステム管理者への通報手順があらかじめ定められていますか？ | | ● | | |
| | バックアップ手順 | 4- 8- 1- 3- 11 | Q システム遮断、ユーザへの緊急サービス停止などのバックアップ手順があらかじめ定められていますか？ | | ● | | |
| | 危機障害発生時の適用業務優先順位 | 4- 8- 1- 3- 12 | Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？ | | ● | | |
| | 障害切り分け | 4- 8- 1- 3- 13 | Q 障害切り分けのために必要な設備を整備していますか？ | | ● | | |
| | 障害発生アラーム | 4- 8- 1- 3- 14 | Q ネットワークを含むシステム全体の運用監視で、障害発生時に運用スタッフに知らせることのできるアラーム等を整備していますか？ | | ● | | |
| | 障害管理票 | 4- 8- 1- 3- 15 | Q すべての障害についての障害管理票の作成要領を定めていますか？ | | ● | | |
| | 定期的評価、是正改善 | 4- 8- 1- 4 | Q 緊急時対策について不具合があった場合、是正処置をとっていますか？ | | ● | | |
| 4. 復旧計画 | 復旧計画 | 4- 8- 1- 5 | Q 復旧計画は、詳細な手続きが定められていますか？ | | ● | ● | |
| | 復旧オーナ、管理者の選定 | 4- 8- 1- 5- 1 | Q 主幹システム、重要ビジネスプロセスごとの、復旧のオーナ、支援のためのシステム管理者、その他の支援スタッフを決めていますか？ | | ● | | |
| | 代替手段 | 4- 8- 1- 5- 2 | Q 代替手段によるバックアップ実施を決定していますか？ | | ● | | |
| | 計画維持・テストのスケジュール化 | 4- 8- 1- 5- 3 | Q 計画の維持、テストのためのスケジュールを決定していますか？ | | ● | | |

## 参考資料

### 情報セキュリティ関連のＵＲＬ

（順不同）

・内閣（ＩＴ戦略本部）　http://www.kantei.go.jp/jp/singi/it2/index.html
・経済産業省（ＭＥＴＩ）　http://www.meti.go.jp
・警視庁（ＮＰＡ）　http://www.npa.go.jp
・総務省（ＭＨＡ）　http://www.soumu.go.jp/
・金融庁（ＦＳＡ）　http://www.fsa.go.jp/
・日本工業標準調査会（ＪＩＳＣ）　http://www.jisc.go.jp/
・情報処理振興事業協会（ＩＰＡ）　http://www.ipa.go.jp
・（財）日本情報処理開発協会（ＪＩＰＤＥＣ）　http://www.jipdec.jp
・有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）
　http://www.jpcert.or.jp
・電子商取引推進協議会（ＥＣＯＭ）　http://www.ecom.or.jp
・（財）日本規格協会（ＪＳＡ）　http://www.jsa.or.jp
・（財）金融情報システムセンター（ＦＩＳＣ）　http://www.fisc.or.jp
・（社）情報サービス産業協会（ＪＩＳＡ）http://www.jisa.or.jp
・システム監査学会（ＪＳＳＡ）　http://www.sysaudit.gr.jp
・情報システム・コントロール協会（ＩＳＡＣＡ）
　東京支部　http://www.isaca.gr.jp/homepage_j.htm
　大阪支部　http://www.isaca-osaka.org
・ＮＰＯ日本システム監査人協会（ＳＡＡＪ）　http://www.saaj.or.jp
・情報処理学会（ＩＰＳＪ）　http://www.ipsj.or.jp
・（社）電子情報技術産業協会（ＪＥＩＴＡ）　http://www.jeita.or.jp
・（社）日本情報システム・ユーザー協会（ＪＵＡＳ）
　http://www.juas.or.jp
・（財）日本品質保証機構（ＪＱＡ）　http:www.jqa.or.jp

・Organization for Economic Co-operation and Development（ＯＥＣＤ）
　http://www.oecd.org
・Bank of International Settlements
・Basel Committee on Banking Supervision
　http://www.bis.org/
・British Standards Institution（ＢＳＩ）
　http://www.bsi-global.com/index.xalter
・National Institute of Standards and Technology（ＮＩＳＴ）
　http://www.nist.gov
・NIST SP 800-12, An Introduction to Computer Society
　http://csrc.nist.gov/publications/nistpubs/800-12 のサイトを参照
・Government of Canada Privy Council Office（ＰＣＯ）カナダ大蔵省
　http://www.pco-bcp.gc.ca/default.asp?Language=e&Page=Home

・Bundesamt für Sicherheit in der Imformationstechnik (BSI) ドイツ情報技術安全局 (Federal Office for Securty in the Information Technology)
http://www.bsi.de/index.htm
・The CERT® Coordination Center (CERT/CC)
http://www.cert.org
・Computer Operations, Audit, and Security Technology (COAST)
http://www.cerias.purdue.edu/coast/coast.html
・Federal Government's Chief Information Officers(CIO) Council
http://bsp.cio.gov
・Forum of Incident Response and Security Teams
http://www.first.org
・"The Information Systems Audit and Control Association & Foundation"
http://www.isaca.org/isacafx.htm
・Internet Security Systems (ISS) Corporate
http://www.iss.net
・The Risk and Insurance Management Society, Inc. (RIMS)
http://www.rims.org
・IT Governance Portal
http://www.itgovernance.org/index.htm
・Information Security Forum
http://www.securityforum.org/html/frameset.htm
・IFAC - The International Federation of Accountants
http://www.ifac.org/
・The Institute of Internal Auditors (The IIA) - Progress Through Sharing
http://www.theiia.org/iia/index.cfm

・Risk Management Magazine
http://www.rmmag.com
・The SANS (System Administration, Networking, and Security) Institute
http://www.sans.org/newlook/home.htm
・TruSecure® Corporation (旧ＩＣＳＡ社)
http://www.trusecure.com

平成15年3月発行

発行所　財団法人　日本情報処理開発協会
東京都港区芝公園3丁目5番8号
機械振興会館内
ＴＥＬ　03(3432)９３８７

印刷所　株式会社　美　行　企　画
東京都千代田区神田錦町2丁目5番地
鈴木第2ビル　2Ｆ
ＴＥＬ　03(3219)２９７１

H14-H003